(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002164938 A**

(43) Date of publication of application: **07.06.02**

(51) Int. Cl **H04L 12/66**
G06F 13/00
H04L 12/56

(21) Application number: **2001274016**

(22) Date of filing: **10.09.01**

(30) Priority: **12.09.00 JP 2000276919**
12.09.00 JP 2000276920

(71) Applicant: **NIPPON TELEGR & TELEPH CORP <NTT>**

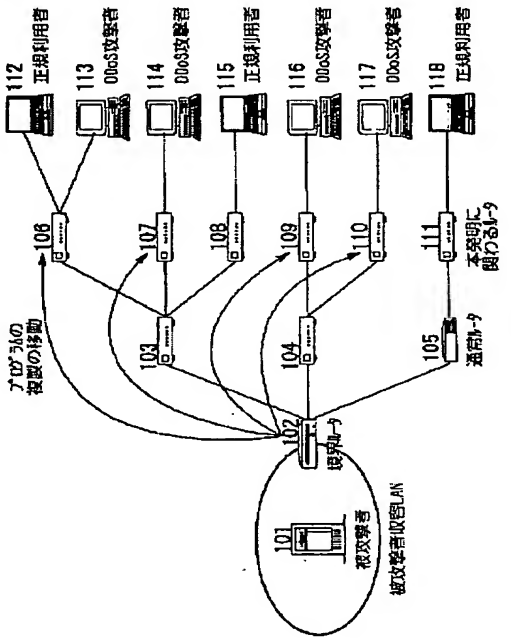
(72) Inventor: **ERIC CHEN**
FUJI HITOSHI

(54) METHOD AND SYSTEM FOR PREVENTING DISTRIBUTION TYPE DENIAL OF SERVICE ATTACK AND ITS COMPUTER PROGRAM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a device and method for preventing a denial of service attack that can protect itself against the denial of service attack independently of whether or not a sender address is arrogated and to provide a computer program.

SOLUTION: A mobile packet filtering program of this invention installed in a border router 102 generates a copy of its own program and moves the copy to routers 106, 107, 109, 110. The mobile packet filtering program moved to each router do not pass all traffics sent from hosts 113, 114, 116, 117 of distribution type DoS(Denial of Service) attackers to a server 101. When the attack is finished, the mobile packet filtering program deletes itself.



(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２００２－１６４９３８
（Ｐ２００２－１６４９３８Ａ）
(43)公開日　平成14年6月7日(2002.6.7)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｈ０４Ｌ	12/66		Ｈ０４Ｌ	12/66	Ｂ	5B089
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１　Ｚ	5K030
Ｈ０４Ｌ	12/56	１００	Ｈ０４Ｌ	12/56	１００　Ｚ	

審査請求　有　請求項の数２１　ＯＬ　（全２５頁）

(21)出願番号　特願2001-274016(P2001-274016)

(22)出願日　平成13年9月10日(2001.9.10)

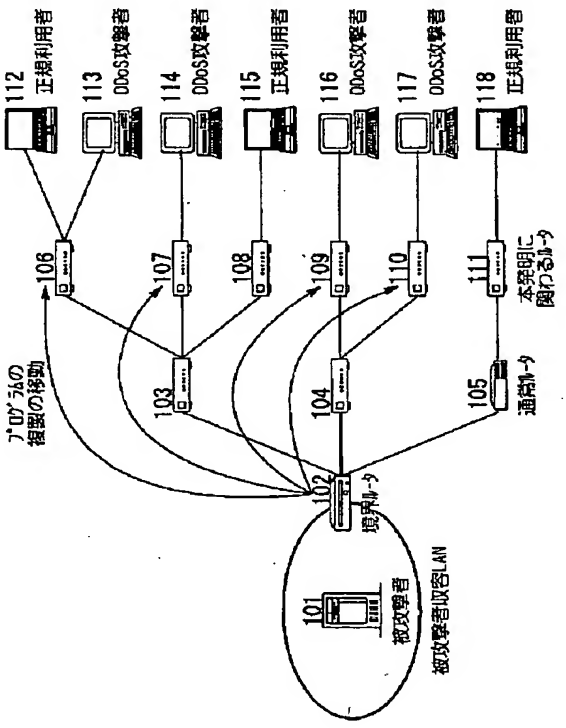
(31)優先権主張番号　特願2000-276919(P2000-276919)
(32)優先日　平成12年9月12日(2000.9.12)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2000-276920(P2000-276920)
(32)優先日　平成12年9月12日(2000.9.12)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号
(72)発明者　エリック・チェン
東京都千代田区大手町二丁目3番1号　日本電信電話株式会社内
(72)発明者　冨士　仁
東京都千代田区大手町二丁目3番1号　日本電信電話株式会社内
(74)代理人　100064908
弁理士　志賀　正武　（外2名）

最終頁に続く

(54)【発明の名称】分散型サービス不能攻撃の防止方法および装置ならびにそのコンピュータプログラム

(57)【要約】
【課題】　送信元アドレスの詐称の如何に関わらず、攻撃を防御できる分散サービス不能攻撃の防止装置および防止方法ならびにそのコンピュータプログラムを提供する。
【解決手段】　境界ルータ１０２にインストールされている本発明の移動型パケットフィルタリングプログラムは、自らのプログラムの複製を作成し、その複製をルータ１０６、１０７、１０９、１１０へ移動させる。各ルータへ移動してきた移動型パケットフィルタリングプログラムは、それぞれ分散型ＤｏＳ攻撃者のホスト１１３、１１４、１１６、１１７からサーバ１０１に向けて送られているトラフィック全てを通過させないようにする。その後、攻撃が終了すると、上記の移動型パケットフィルタリングのプログラムは、自分自身を消去する。



1

【特許請求の範囲】

【請求項１】　分散型サービス不能攻撃を防止するための通信装置であって、

当該通信装置を通過する通信パケットを監視し分散型サービス不能攻撃を検出するトラフィック監視機能部と、

分散型サービス不能攻撃が検出された際に当該分散型サービス不能攻撃の通信パケットを破棄する攻撃防御モジュールと、

攻撃元に近い上位側の通信装置のアドレスを検索する処理を行う攻撃元検索モジュールと、

上位側の防御位置の通信装置に対して前記攻撃元検索モジュールを送信するモジュール送信部と、

前記攻撃元検索モジュールによって検索された攻撃元に近い上位側の通信装置の候補中から上位側の防御位置とする通信装置を抽出する攻撃元判断機能部とを備え、

前記モジュール送信部は、前記攻撃元判断機能部によって抽出された上位側の防御位置の通信装置に対して前記攻撃防御モジュールを送信するものであることを特徴とする通信装置。

【請求項２】　請求項１に記載の通信装置であって、

前記モジュール送信部は、前記攻撃元検索モジュールとともに前記トラフィック監視機能部によって分散型サービス不能攻撃であると検知された通信パケットに関する攻撃パケット情報を前記上位側の通信装置に対して送信するものであり、

前記攻撃元検索モジュールには、前記モジュール送信部から受信した前記攻撃パケット情報と当該通信装置を通過する通信パケットとを比較して、当該攻撃パケット情報に該当する通信パケットが当該通信装置を通過していることを検知した場合には、当該通信装置自身が防御位置の通信装置の候補であることを送信元の通信装置に対して通知するトラフィック検査機能部が含まれることを特徴とする通信装置。

【請求項３】　請求項１に記載の通信装置であって、

前記攻撃防御モジュールには、

攻撃が継続中か否かを監視する攻撃トラフィック監視機能部と、

前記攻撃トラフィック監視機能部が攻撃は中断したと判断した場合には、当該攻撃防御モジュール自身を、処理実行中の通信装置から消滅させる自己消滅機能部とが含まれることを特徴とする通信装置。

【請求項４】　請求項１から３までのいずれかに記載の通信装置と、

前記通信装置に対してプログラムモジュールを送信するモジュールサーバであって、

前記通信装置にインストールされるプログラムモジュールを保存するプログラムモジュールデータベースと、

前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を管理する開発者データベースと、

2

前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者を管理するユーザデータベースと、

保存されている前記プログラムモジュールを前記利用者にメニューで表示するサービスメニューと、

前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあれば前記利用者の権限を認証するサービスマネージャと、

前記認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信するサービスモジュールインジェクタと、

を備えるモジュールサーバと、

からなることを特徴とする通信システム。

【請求項５】　分散型サービス不能攻撃を防止するための通信装置であって、

当該通信装置を通過する通信パケットを監視し分散型サービス不能攻撃を検出するトラフィック監視機能部と、

分散型サービス不能攻撃が検出された際に当該分散型サービス不能攻撃の通信パケットを破棄するとともに、攻撃元に近い上位側の通信装置のアドレスを検索する処理を行う攻撃防御モジュールと、

上位側の通信装置に対して前記攻撃防御モジュールを送信するモジュール送信部と、

を備えることを特徴とする通信装置。

【請求項６】　請求項５に記載の通信装置であって、

前記モジュール送信部は、前記攻撃防御モジュールとともに前記トラフィック監視機能部によって分散型サービス不能攻撃であると検知された通信パケットに関する攻撃パケット情報を前記上位側の通信装置に対して送信するものであり、

前記攻撃防御モジュールには、前記モジュール送信部から受信した前記攻撃パケット情報と当該通信装置を通過する通信パケットとを比較して、当該攻撃パケット情報に該当する通信パケットが当該通信装置を通過していることを検知するトラフィック検査機能部が含まれることを特徴とする通信装置。

【請求項７】　請求項５に記載の通信装置であって、

前記攻撃防御モジュールには、

攻撃が継続中か否かを監視する攻撃トラフィック監視機能部と、

前記攻撃トラフィック監視機能部が攻撃は中断したと判断した場合には、当該攻撃防御モジュール自身を、処理実行中の通信装置から消滅させる自己消滅機能部とが含まれることを特徴とする通信装置。

【請求項８】　請求項５から７までのいずれかに記載の通信装置と、

前記通信装置に対してプログラムモジュールを送信するモジュールサーバであって、

前記通信装置にインストールされるプログラムモジュー

ルを保存するプログラムモジュールデータベースと、
前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を管理する開発者データベースと、
前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者を管理するユーザデータベースと、
保存されている前記プログラムモジュールを前記利用者にメニューで表示するサービスメニューと、
前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあれば前記利用者の権限を認証するサービスマネージャと、
前記認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信するサービスモジュールインジェクタと、
を備えるモジュールサーバと、
からなることを特徴とする通信システム。

【請求項９】　分散型サービス不能攻撃を防止するためのサービス不能攻撃防止方法であって、
通信装置において分散型サービス不能攻撃を検知すると、当該分散型サービス不能攻撃の通信パケットを当該通信装置において破棄しながら、
検知された前記分散型サービス不能攻撃の攻撃元に近い上位側の通信装置を検索し、
検索の結果得られた前記上位側の通信装置に対してプログラムモジュールを送信し、
前記プログラムモジュールを受信した側の通信装置において、当該プログラムモジュールを実行することにより、上記の分散型サービス不能攻撃の通信パケットを破棄する処理と、上記の上位側の通信サービスを検索する処理と、上記の上位側の通信装置に対してプログラムモジュールを送信する処理を行うことによって、
攻撃元に最も近い最上位の通信装置に達するまで再帰的に検索を行い、当該最上位の通信装置において前記分散型サービス不能攻撃の通信パケットを破棄することを特徴とするサービス不能攻撃防止方法。

【請求項１０】　請求項９に記載のサービス不能攻撃防止方法であって、
前記プログラムモジュールを上位側の通信装置に対して送信する際には、前記プログラムモジュールとともに、分散型サービス不能攻撃であると検知された前記通信パケットに関する攻撃パケット情報を前記上位側の通信装置に対して送信し、
前記プログラムモジュールと前記攻撃パケット情報を受信した側の通信装置では、当該プログラムモジュールを実行することによって、前記攻撃パケット情報と当該通信装置を通過する通信パケットとを比較して、当該攻撃パケット情報に該当する通信パケットが当該通信装置を通過していることを検知した場合には、当該通信装置自身が防御位置の通信装置の候補であることを送信元の通信装置に対して通知することを特徴とするサービス不能攻撃防止方法。

【請求項１１】　請求項９に記載のサービス不能攻撃防止方法であって、
前記プログラムモジュールを受信した前記上位側の通信装置においては、当該プログラムモジュールを実行することによって、攻撃が継続中か否かを監視するとともに、この攻撃が中断された判断した場合には、当該プログラムモジュール自身を当該通信装置から消滅させる処理を行うことを特徴とするサービス不能攻撃防止方法。

【請求項１２】　分散型サービス不能攻撃を防止するために通信装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、
前記通信装置を通過する通信パケットを監視するステップと、
この監視によってサービス不能攻撃の通信パケットを検知した場合には、当該サービス不能攻撃の通信パケットを継続的に破棄する処理を行うステップと、前記サービス不能攻撃が分散型のサービス不能攻撃であるか否かを判断するステップと、
分散型のサービス不能攻撃であった場合には、データベースを参照することによって攻撃元に近い上位側の通信装置を抽出し、これらの上位側の通信装置に対して攻撃元を検索するための攻撃元検索モジュールを送信し、送信先の通信装置から防御位置の情報を受信し、この防御位置の情報に基づいて上位側の通信装置に対して攻撃を防御するための攻撃防御モジュールを送信するステップと、
の各処理をコンピュータに実行させるコンピュータプログラムを記録した記録媒体。

【請求項１３】　分散型サービス不能攻撃を防止するために下位の通信装置から上位の通信装置へ送信され、この上位の通信装置上で実行される攻撃元検索のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、
当該通信装置を通過する通信パケットと、サービス不能攻撃に関する攻撃パケット情報とを比較して、当該サービス不能攻撃の通信パケットが当該通信装置を通過しているか否かを検査し、この検査結果を前記下位の通信装置に通知するステップと、
この検査の結果、当該サービス不能攻撃の通信パケットが当該通信装置を通過している場合には、
ａ）自通信装置自身よりも攻撃元に近い上位の通信装置がない場合には当該通信装置自身を最上位の通信装置として前記下位の通信装置に通知する、
ｂ）自該通信装置自身よりも攻撃元に近い上位の通信装置がある場合であり、この上位の通信装置に対して当該攻撃元検索のコンピュータプログラムを送信した結果、

この上位の通信装置から当該サービス不能攻撃の通信パケットが通過しているという通知が一個も来ない場合には、自通信装置自身を最上位の通信装置として前記下位の通信装置に通知する、
ｃ）自該通信装置自身よりも攻撃元に近い上位の通信装置がある場合であり、この上位の通信装置に対して当該攻撃元検索のコンピュータプログラムを送信した結果、この上位の通信装置から当該サービス不能攻撃の通信パケットが通過しているという通知が一個以上来た場合には、自通信装置自身を最上位の通信装置としない、
のａ）～ｃ）のいずれかを行うステップと、
の各処理をコンピュータに実行させるコンピュータプログラムを記録した記録媒体。
【請求項１４】分散型サービス不能攻撃を防止するために通信装置上で実行される攻撃防御のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、
当該通信装置を通過する通信パケットと、サービス不能攻撃に関する攻撃パケット情報とを比較して、当該サービス不能攻撃の通信パケットが当該通信装置を通過しているか否かを検査し、この検査結果、通過していた場合には、
ａ）当該サービス不能攻撃の通信パケットを継続的に破棄する処理を行うステップと、
ｂ）データベースを参照することによって攻撃元に近い上位側の通信装置を抽出するステップと、
ｃ）抽出された前記上位側の通信装置に対して当該攻撃防御のコンピュータプログラム自身を送信するステップと、
のａ）～ｃ）の各処理をコンピュータに実行させるコンピュータプログラムを記録した記録媒体。
【請求項１５】　分散型サービス不能攻撃を防止するために通信装置上で実行されるコンピュータプログラムであって、
前記通信装置を通過する通信パケットを監視するステップと、
この監視によってサービス不能攻撃の通信パケットを検知した場合には、当該サービス不能攻撃の通信パケットを継続的に破棄する処理を行うステップと、
前記サービス不能攻撃が分散型のサービス不能攻撃であるか否かを判断するステップと、
分散型のサービス不能攻撃であった場合には、データベースを参照することによって攻撃元に近い上位側の通信装置を抽出し、これらの上位側の通信装置に対して攻撃元を検索するための攻撃元検索モジュールを送信し、送信先の通信装置から防御位置の情報を受信し、この防御位置の情報に基づいて上位側の通信装置に対して攻撃を防御するための攻撃防御モジュールを送信するステップと、
の各処理をコンピュータに実行させるコンピュータプログラム。
【請求項１６】　分散型サービス不能攻撃を防止するために下位の通信装置から上位の通信装置へ送信され、この上位の通信装置上で実行される攻撃元検索のコンピュータプログラムであって、
当該通信装置を通過する通信パケットと、サービス不能攻撃に関する攻撃パケット情報とを比較して、当該サービス不能攻撃の通信パケットが当該通信装置を通過しているか否かを検査し、この検査結果を前記下位の通信装置に通知するステップと、
この検査の結果、当該サービス不能攻撃の通信パケットが当該通信装置を通過している場合には、
ａ）自通信装置自身よりも攻撃元に近い上位の通信装置がない場合には当該通信装置自身を最上位の通信装置として前記下位の通信装置に通知する、
ｂ）自該通信装置自身よりも攻撃元に近い上位の通信装置がある場合であり、この上位の通信装置に対して当該攻撃元検索のコンピュータプログラムを送信した結果、この上位の通信装置から当該サービス不能攻撃の通信パケットが通過しているという通知が一個も来ない場合には、自通信装置自身を最上位の通信装置として前記下位の通信装置に通知する、
ｃ）自該通信装置自身よりも攻撃元に近い上位の通信装置がある場合であり、この上位の通信装置に対して当該攻撃元検索のコンピュータプログラムを送信した結果、この上位の通信装置から当該サービス不能攻撃の通信パケットが通過しているという通知が一個以上来た場合には、自通信装置自身を最上位の通信装置としない、
のａ）～ｃ）のいずれかを行うステップと、
の各処理をコンピュータに実行させるコンピュータプログラム。
【請求項１７】分散型サービス不能攻撃を防止するために通信装置上で実行される攻撃防御のコンピュータプログラムであって、
当該通信装置を通過する通信パケットと、サービス不能攻撃に関する攻撃パケット情報とを比較して、当該サービス不能攻撃の通信パケットが当該通信装置を通過しているか否かを検査し、この検査結果、通過していた場合には、
ａ）当該サービス不能攻撃の通信パケットを継続的に破棄する処理を行うステップと、
ｂ）データベースを参照することによって攻撃元に近い上位側の通信装置を抽出するステップと、
ｃ）抽出された前記上位側の通信装置に対して当該攻撃防御のコンピュータプログラム自身を送信するステップと、
のａ）～ｃ）の各処理をコンピュータに実行させるコンピュータプログラム。
【請求項１８】　通信装置に対してプログラムモジュールを送信するモジュールサーバであって、

前記通信装置にインストールされるプログラムモジュールを保存するプログラムモジュールデータベースと、
前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を管理する開発者データベースと、
前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者を管理するユーザデータベースと、
保存されている前記プログラムモジュールを前記利用者にメニューで表示するサービスメニューと、
前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあれば前記利用者の権限を認証するサービスマネージャと、
前記認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信するサービスモジュールインジェクタと、
を備えることを特徴とするモジュールサーバ。

【請求項１９】　通信装置上でプログラムモジュールを実行させるためのモジュール提供方法であって、
前記通信装置にインストールされる前記プログラムモジュールをプログラムモジュールデータベースに保存する第１の過程と、
前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を開発者データベースで管理する第２の過程と、
前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者をユーザデータベースで管理する第３の過程と、
前記第１の過程において保存された前記プログラムモジュールを前記利用者にサービスメニューに含めて表示する第４の過程と、
前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあった際に前記利用者の権限を認証する第５の過程と、
前記第５の過程において認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信する第６の過程とを有することを特徴とするモジュール提供方法。

【請求項２０】　通信装置上でプログラムモジュールを実行させるためのモジュール提供処理をコンピュータに実行させるコンピュータプログラムであって、
前記通信装置にインストールされる前記プログラムモジュールをプログラムモジュールデータベースに保存する第１のステップと、
前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を開発者データベースで管理する第２のステップと、
前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者をユーザデータベースで管理する第３のステップと、
前記第１のステップにおいて保存された前記プログラムモジュールを前記利用者にサービスメニューに含めて表示する第４のステップと、
前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあった際に前記利用者の権限を認証する第５のステップと、
前記第５のステップにおいて認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信する第６のステップとの各ステップの処理をコンピュータに実行させるコンピュータプログラム。

【請求項２１】　通信装置上でプログラムモジュールを実行させるためのモジュール提供処理をコンピュータに実行させるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、
前記通信装置にインストールされる前記プログラムモジュールをプログラムモジュールデータベースに保存する第１のステップと、
前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を開発者データベースで管理する第２のステップと、
前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者をユーザデータベースで管理する第３のステップと、
前記第１のステップにおいて保存された前記プログラムモジュールを前記利用者にサービスメニューに含めて表示する第４のステップと、
前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあった際に前記利用者の権限を認証する第５のステップと、
前記第５のステップにおいて認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信する第６のステップとの各ステップの処理をコンピュータに実行させるコンピュータプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークに接続された機器をネットワーク経由での攻撃から防御するための、サービス不能攻撃の防止方法およびその装置ならびにそのコンピュータプログラムに関するものである。

【０００２】

【従来の技術】従来、ＴＣＰ／ＩＰ（Transmission control protocol/internet protocol）などのネットワークプロトコルは、オープンとなっており、互いに信用されるグループで使われるように設計されている。このため、コンピュータのオペレーティングシステムでは、大

量の通信トラフィック（データ等）をサーバに送信することによって、ネットワークの帯域やサーバの資源を消費して正当な利用者の利用を妨げようとするサービス不能攻撃（以下、「ＤｏＳ（Denial of Service）攻撃」と記す）を防ぐことは考慮されていない。このようなＤｏＳ攻撃に対する防御の方法は増えてきているが、複数箇所から同時に連携してＤｏＳ攻撃を行う分散型サービス不能攻撃（ＤＤｏＳ攻撃）に対する防御の方法は未だ効果的ではない。

【０００３】この分散型ＤｏＳ攻撃に対する防御の方法としては、シスコ社が提案したＩｎｇｒｅｓｓ　Ｆｉｌｔｅｒ（ＲＦＣ２２６７）とＵＵＮＥＴ社のＣｅｎｔｅｒＴｒａｃｋがある。前者は、分散型ＤｏＳ攻撃の際に良く使われる送信元アドレスの詐称をチェックする機構であり、ローカルエリアネットワークがインターネットに接続されている境界であるルータにインストールされ、ローカルエリアネットワークからインターネットに向かって送信されるパケットの送信元アドレスの正統性をチェックし、ローカルエリアネットワークに割り当てられたアドレスと整合していない場合には、そのパケットをインターネットに送信せずに破棄する。

【０００４】

【発明が解決しようとする課題】この技術は、送信元アドレスを詐称して分散型ＤｏＳ攻撃をすることを禁止するための技術であり、攻撃を受ける側が防御するために使う技術ではない。また後者は、インターネットのルータに診断機能を付加し、分散型ＤｏＳ攻撃の送信元を追跡する技術である。この技術は、攻撃を受けた被害者が攻撃者を特定することを助ける技術ではあるが、実際に攻撃を受けているときにその攻撃を防御することはできない。

【０００５】上述したＲＦＣ２２６７に記載されているＩｎｇｒｅｓｓ　Ｆｉｌｔｅｒは、正しいＩＰ（internet protocol）アドレスが送信元になっているＩＰパケットによる攻撃にはまったく対処できない、攻撃元になっているローカルエリアネットワークとインターネットとの境界であるルータにＩｎｇｒｅｓｓ　Ｆｉｌｔｅｒが具備されていない場合はまったく攻撃の防御に役に立たないという問題点がある。また、上述したＣｅｎｔｅｒ　Ｔｒａｃｋは、攻撃者が送信元アドレスを詐称した場合には追跡が困難になる上に、複数箇所に分散された分散型ＤｏＳの攻撃元になっているコンピュータやそのコンピュータが接続されているネットワークの管理者に連絡をしないと、攻撃そのものを止めることはできないため、実質的には攻撃を止めるまでに何時間、あるいは何日もの時間がかかってしまうという問題点がある。

【０００６】本発明は、上記事情を考慮してなされたものであり、その目的は、送信元アドレスを詐称したパケットによる分散型ＤｏＳ攻撃を防御する際に、送信元アドレスの詐称の如何に関わらず、攻撃を防御できる分散サービス不能攻撃の防止装置および防止方法ならびにそのコンピュータプログラムを提供することである。

【０００７】また、本発明の目的は、上記の分散サービス不能攻撃の防止方法を実現するために、通信装置に対して送信するためのプログラムモジュールを管理するとともに、プログラムモジュールの開発者や利用者らの認証を行い、通信システム全体の信頼性を向上させることのできるモジュールサーバを提供することである。

【０００８】

【課題を解決するための手段】上記の課題を解決するために、本発明は、分散型サービス不能攻撃を防止するための通信装置であって、当該通信装置を通過する通信パケットを監視し分散型サービス不能攻撃を検出するトラフィック監視機能部と、分散型サービス不能攻撃が検出された際に当該分散型サービス不能攻撃の通信パケットを破棄する攻撃防御モジュールと、攻撃元に近い上位側の通信装置のアドレスを検索する処理を行う攻撃元検索モジュールと、上位側の防御位置の通信装置に対して前記攻撃元検索モジュールを送信するモジュール送信部と、前記攻撃元検索モジュールによって検索された攻撃元に近い上位側の通信装置の候補中から上位側の防御位置とする通信装置を抽出する攻撃元判断機能部とを備え、前記モジュール送信部は、前記攻撃元判断機能部によって抽出された上位側の防御位置の通信装置に対して前記攻撃防御モジュールを送信するものであることを特徴とする通信装置を要旨とする。

【０００９】また、本発明の通信装置においては、前記モジュール送信部は、前記攻撃元検索モジュールとともに前記トラフィック監視機能部によって分散型サービス不能攻撃であると検知された通信パケットに関する攻撃パケット情報を前記上位側の通信装置に対して送信するものであり、前記攻撃元検索モジュールには、前記モジュール送信部から受信した前記攻撃パケット情報と当該通信装置を通過する通信パケットとを比較して、当該攻撃パケット情報に該当する通信パケットが当該通信装置を通過していることを検知した場合には、当該通信装置自身が防御位置の通信装置の候補であることを送信元の通信装置に対して通知するトラフィック検査機能部が含まれることを特徴とする。

【００１０】また、本発明の通信装置においては、前記攻撃防御モジュールには、攻撃が継続中か否かを監視する攻撃トラフィック監視機能部と、前記攻撃トラフィック監視機能部が攻撃は中断したと判断した場合には、当該攻撃防御モジュール自身を、処理実行中の通信装置から消滅させる自己消滅機能部とが含まれることを特徴とする。

【００１１】また、本発明の通信システムは、上記の通信装置と、前記通信装置に対してプログラムモジュールを送信するモジュールサーバであって、前記通信装置にインストールされるプログラムモジュールを保存するプ

ログラムモジュールデータベースと、前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を管理する開発者データベースと、前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者を管理するユーザデータベースと、保存されている前記プログラムモジュールを前記利用者にメニューで表示するサービスメニューと、前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあれば前記利用者の権限を認証するサービスマネージャと、前記認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信するサービスモジュールインジェクタとを備えるモジュールサーバと、からなることを特徴とするものである。

【００１２】また、本発明の通信装置は、当該通信装置を通過する通信パケットを監視し分散型サービス不能攻撃を検出するトラフィック監視機能部と、分散型サービス不能攻撃が検出された際に当該分散型サービス不能攻撃の通信パケットを破棄するとともに、攻撃元に近い上位側の通信装置のアドレスを検索する処理を行う攻撃防御モジュールと、上位側の通信装置に対して前記攻撃防御モジュールを送信するモジュール送信部とを備えることを特徴とするものである。

【００１３】また、本発明の通信装置においては、前記モジュール送信部は、前記攻撃防御モジュールとともに前記トラフィック監視機能部によって分散型サービス不能攻撃であると検知された通信パケットに関する攻撃パケット情報を前記上位側の通信装置に対して送信するものであり、前記攻撃防御モジュールには、前記モジュール送信部から受信した前記攻撃パケット情報と当該通信装置を通過する通信パケットとを比較して、当該攻撃パケット情報に該当する通信パケットが当該通信装置を通過していることを検知するトラフィック検査機能部が含まれることを特徴とする。

【００１４】また、本発明の通信装置においては、前記攻撃防御モジュールには、攻撃が継続中か否かを監視する攻撃トラフィック監視機能部と、前記攻撃トラフィック監視機能部が攻撃は中断したと判断した場合には、当該攻撃防御モジュール自身を、処理実行中の通信装置から消滅させる自己消滅機能部とが含まれることを特徴とする。

【００１５】また、本発明の通信システムは、上記の通信装置と、前記通信装置に対してプログラムモジュールを送信するモジュールサーバであって、前記通信装置にインストールされるプログラムモジュールを保存するプログラムモジュールデータベースと、前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を管理する開発者データベースと、前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者を管理するユーザデータベースと、保存されている前記プログラムモジュールを前記利用者にメニューで表示するサービスメニューと、前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあれば前記利用者の権限を認証するサービスマネージャと、前記認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信するサービスモジュールインジェクタとを備えるモジュールサーバと、からなることを特徴とするものである。

【００１６】また、本発明のサービス不能攻撃防止方法は、通信装置において分散型サービス不能攻撃を検知すると、当該分散型サービス不能攻撃の通信パケットを当該通信装置において破棄しながら、検知された前記分散型サービス不能攻撃の攻撃元に近い上位側の通信装置を検索し、検索の結果得られた前記上位側の通信装置に対してプログラムモジュールを送信し、前記プログラムモジュールを受信した側の通信装置において、当該プログラムモジュールを実行することにより、上記の分散型サービス不能攻撃の通信パケットを破棄する処理と、上記の上位側の通信サービスを検索する処理と、上記の上位側の通信装置に対してプログラムモジュールを送信する処理を行うことによって、攻撃元に最も近い最上位の通信装置に達するまで再帰的に検索を行い、当該最上位の通信装置において前記分散型サービス不能攻撃の通信パケットを破棄することを特徴とするものである。

【００１７】また、本発明のサービス不能攻撃防止方法では、前記プログラムモジュールを上位側の通信装置に対して送信する際には、前記プログラムモジュールとともに、分散型サービス不能攻撃であると検知された前記通信パケットに関する攻撃パケット情報を前記上位側の通信装置に対して送信し、前記プログラムモジュールと前記攻撃パケット情報を受信した側の通信装置では、当該プログラムモジュールを実行することによって、前記攻撃パケット情報と当該通信装置を通過する通信パケットとを比較して、当該攻撃パケット情報に該当する通信パケットが当該通信装置を通過していることを検知した場合には、当該通信装置自身が防御位置の通信装置の候補であることを送信元の通信装置に対して通知することを特徴とする。

【００１８】また、本発明のサービス不能攻撃防止方法では、前記プログラムモジュールを受信した前記上位側の通信装置においては、当該プログラムモジュールを実行することによって、攻撃が継続中か否かを監視するとともに、この攻撃が中断された判断した場合には、当該プログラムモジュール自身を当該通信装置から消滅させる処理を行うことを特徴とする。

【００１９】また、本発明の記録媒体は、分散型サービス不能攻撃を防止するために通信装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体は、前記通信装置を通過する通信パケッ

トを監視するステップと、この監視によってサービス不能攻撃の通信パケットを検知した場合には、当該サービス不能攻撃の通信パケットを継続的に破棄する処理を行うステップと、前記サービス不能攻撃が分散型のサービス不能攻撃であるか否かを判断するステップと、分散型のサービス不能攻撃であった場合には、データベースを参照することによって攻撃元に近い上位側の通信装置を抽出し、これらの上位側の通信装置に対して攻撃元を検索するための攻撃元検索モジュールを送信し、送信先の通信装置から防御位置の情報を受信し、この防御位置の情報に基づいて上位側の通信装置に対して攻撃を防御するための攻撃防御モジュールを送信するステップとの各処理をコンピュータに実行させるコンピュータプログラムを記録したものである。

【００２０】また、本発明の記録媒体は、分散型サービス不能攻撃を防止するために下位の通信装置から上位の通信装置へ送信され、この上位の通信装置上で実行される攻撃元検索のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、当該通信装置を通過する通信パケットと、サービス不能攻撃に関する攻撃パケット情報とを比較して、当該サービス不能攻撃の通信パケットが当該通信装置を通過しているか否かを検査し、この検査結果を前記下位の通信装置に通知するステップと、この検査の結果、当該サービス不能攻撃の通信パケットが当該通信装置を通過している場合には、

ａ）自通信装置自身よりも攻撃元に近い上位の通信装置がない場合には当該通信装置自身を最上位の通信装置として前記下位の通信装置に通知する、

ｂ）自該通信装置自身よりも攻撃元に近い上位の通信装置がある場合であり、この上位の通信装置に対して当該攻撃元検索のコンピュータプログラムを送信した結果、この上位の通信装置から当該サービス不能攻撃の通信パケットが通過しているという通知が一個も来ない場合には、自通信装置自身を最上位の通信装置として前記下位の通信装置に通知する、

ｃ）自該通信装置自身よりも攻撃元に近い上位の通信装置がある場合であり、この上位の通信装置に対して当該攻撃元検索のコンピュータプログラムを送信した結果、この上位の通信装置から当該サービス不能攻撃の通信パケットが通過しているという通知が一個以上来た場合には、自通信装置自身を最上位の通信装置としない、のａ）～ｃ）のいずれかを行うステップとの各処理をコンピュータに実行させるコンピュータプログラムを記録したものである。

【００２１】また、本発明の記録媒体は、分散型サービス不能攻撃を防止するために通信装置上で実行される攻撃防御のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、当該通信装置を通過する通信パケットと、サービス不能攻撃に関する攻撃

パケット情報とを比較して、当該サービス不能攻撃の通信パケットが当該通信装置を通過しているか否かを検査し、この検査結果、通過していた場合には、

ａ）当該サービス不能攻撃の通信パケットを継続的に破棄する処理を行うステップと、

ｂ）データベースを参照することによって攻撃元に近い上位側の通信装置を抽出するステップと、

ｃ）抽出された前記上位側の通信装置に対して当該攻撃防御のコンピュータプログラム自身を送信するステップと、のａ）～ｃ）の各処理をコンピュータに実行させるコンピュータプログラムを記録したものである。

【００２２】また、本発明は、分散型サービス不能攻撃を防止するために通信装置上で実行されるコンピュータプログラムであって、前記通信装置を通過する通信パケットを監視するステップと、この監視によってサービス不能攻撃の通信パケットを検知した場合には、当該サービス不能攻撃の通信パケットを継続的に破棄する処理を行うステップと、前記サービス不能攻撃が分散型のサービス不能攻撃であるか否かを判断するステップと、分散型のサービス不能攻撃であった場合には、データベースを参照することによって攻撃元に近い上位側の通信装置を抽出し、これらの上位側の通信装置に対して攻撃元を検索するための攻撃元検索モジュールを送信し、送信先の通信装置から防御位置の情報を受信し、この防御位置の情報に基づいて上位側の通信装置に対して攻撃を防御するための攻撃防御モジュールを送信するステップとの各処理をコンピュータに実行させるものである。

【００２３】また、本発明は、分散型サービス不能攻撃を防止するために下位の通信装置から上位の通信装置へ送信され、この上位の通信装置上で実行される攻撃元検索のコンピュータプログラムであって、当該通信装置を通過する通信パケットと、サービス不能攻撃に関する攻撃パケット情報とを比較して、当該サービス不能攻撃の通信パケットが当該通信装置を通過しているか否かを検査し、この検査結果を前記下位の通信装置に通知するステップと、この検査の結果、当該サービス不能攻撃の通信パケットが当該通信装置を通過している場合には、

ａ）自通信装置自身よりも攻撃元に近い上位の通信装置がない場合には当該通信装置自身を最上位の通信装置として前記下位の通信装置に通知する、

ｂ）自該通信装置自身よりも攻撃元に近い上位の通信装置がある場合であり、この上位の通信装置に対して当該攻撃元検索のコンピュータプログラムを送信した結果、この上位の通信装置から当該サービス不能攻撃の通信パケットが通過しているという通知が一個も来ない場合には、自通信装置自身を最上位の通信装置として前記下位の通信装置に通知する、

ｃ）自該通信装置自身よりも攻撃元に近い上位の通信装置がある場合であり、この上位の通信装置に対して当該攻撃元検索のコンピュータプログラムを送信した結果、

この上位の通信装置から当該サービス不能攻撃の通信パケットが通過しているという通知が一個以上来た場合には、自通信装置自身を最上位の通信装置としない、のａ）～ｃ）のいずれかを行うステップとの各処理をコンピュータに実行させるものである。

【００２４】また、本発明は、分散型サービス不能攻撃を防止するために通信装置上で実行される攻撃防御のコンピュータプログラムであって、当該通信装置を通過する通信パケットと、サービス不能攻撃に関する攻撃パケット情報とを比較して、当該サービス不能攻撃の通信パケットが当該通信装置を通過しているか否かを検査し、この検査結果、通過していた場合には、

ａ）当該サービス不能攻撃の通信パケットを継続的に破棄する処理を行うステップと、

ｂ）データベースを参照することによって攻撃元に近い上位側の通信装置を抽出するステップと、

ｃ）抽出された前記上位側の通信装置に対して当該攻撃防御のコンピュータプログラム自身を送信するステップと、のａ）～ｃ）の各処理をコンピュータに実行させるものである。

【００２５】また、本発明は、通信装置に対してプログラムモジュールを送信するモジュールサーバであって、前記通信装置にインストールされるプログラムモジュールを保存するプログラムモジュールデータベースと、前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を管理する開発者データベースと、前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者を管理するユーザデータベースと、保存されている前記プログラムモジュールを前記利用者にメニューで表示するサービスメニューと、前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあれば前記利用者の権限を認証するサービスマネージャと、前記認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信するサービスモジュールインジェクタとを備えることを特徴とするものである。

【００２６】また、本発明は、通信装置上でプログラムモジュールを実行させるためのモジュール提供方法であって、前記通信装置にインストールされる前記プログラムモジュールをプログラムモジュールデータベースに保存する第１の過程と、前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を開発者データベースで管理する第２の過程と、前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者をユーザデータベースで管理する第３の過程と、前記第１の過程において保存された前記プログラムモジュールを前記利用者にサービスメニューに含めて表示する第４の過程と、前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあった際に前記利用者の権限を認証する第５の過程と、前記第５の過程において認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信する第６の過程とを有することを特徴とするものである。

【００２７】また、本発明のコンピュータプログラムは、前記通信装置にインストールされる前記プログラムモジュールをプログラムモジュールデータベースに保存する第１のステップと、前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を開発者データベースで管理する第２のステップと、前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者をユーザデータベースで管理する第３のステップと、前記第１のステップにおいて保存された前記プログラムモジュールを前記利用者にサービスメニューに含めて表示する第４のステップと、前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあった際に前記利用者の権限を認証する第５のステップと、前記第５のステップにおいて認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信する第６のステップとの各ステップの処理をコンピュータに実行させるものである。

【００２８】また、本発明の記録媒体は、前記通信装置にインストールされる前記プログラムモジュールをプログラムモジュールデータベースに保存する第１のステップと、前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を開発者データベースで管理する第２のステップと、前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者をユーザデータベースで管理する第３のステップと、前記第１のステップにおいて保存された前記プログラムモジュールを前記利用者にサービスメニューに含めて表示する第４のステップと、前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあった際に前記利用者の権限を認証する第５のステップと、前記第５のステップにおいて認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信する第６のステップとの各ステップの処理をコンピュータに実行させるコンピュータプログラムを記録した記録媒体である。

【００２９】

【発明の実施の形態】以下、図面を参照しこの発明の実施形態について説明する。なお、以下の実施形態は本発明の請求範囲の解釈を限定するものではない。また、前記の目的を達成するために、以下の実施形態において説明されるすべての特徴を組み合わせることが常に不可欠であるわけではない。

【００３０】＜第１の実施形態＞以下、本発明の実施の形態について図を用いて詳細に説明する。図１は、本発明を適用できるネットワークの構成図である。分散型Ｄ

ｏＳ攻撃者によって操作されたホスト１１３、１１４、１１６、１１７は、攻撃パケットを被攻撃者のサーバ１０１に向かって送信している。この被攻撃者のサーバ１０１が収容されているローカルエリアネットワーク（ＬＡＮ）は、境界ルータ（通信装置）１０２によって外部のネットワークに接続されており、この境界ルータ１０２には、本発明の移動型パケットフィルタリングがインストールされている。また、ルータ（通信装置）１０３、１０４、１０６、１０７、１０８、１０９、１１０、１１１もまた本発明の技術を適用したルータであり、これらはネットワーク経由で送られてきたプログラムを受信し実行できる機能が備わっている。なお、ルータ１０５は本発明の技術を適用したものではない通常のルータである。

【００３１】図１に示すネットワークにおいて、分散型ＤｏＳ攻撃によって、前記攻撃パケットが被攻撃者収容ＬＡＮに集中して混雑が発生し、これにより、前記境界ルータ１０２の資源を消費してしまい、この混雑によって、分散型ＤｏＳ攻撃者とは無関係な正規の利用者のコンピュータ１１２、１１５、１１８からサーバ１０１に接続できなくなるということが起こる。

【００３２】次に、図２は、図１に示したネットワークにおいて行われている分散型ＤｏＳ攻撃に対しての防御方法を示している。図２の態様では、境界ルータ１０２にインストールされている本発明の移動型パケットフィルタリングプログラムは、自らのプログラムの複製を作成し、その複製を後述する方法によってルータ１０６、１０７、１０９、１１０へ移動させる。各ルータへ移動してきた移動型パケットフィルタリングプログラムは、それぞれ分散型ＤｏＳ攻撃者のホスト１１３、１１４、１１６、１１７からサーバ１０１に向けて送られているトラフィック全てを通過させないようにする。その結果、境界ルータ１０２の負荷が軽減されると共に被攻撃者収容ＬＡＮの混雑が解消され、分散型ＤｏＳ攻撃者以外の正規利用者のコンピュータ１１２、１１５、１１８からサーバ１０１にアクセスできるようになる。その後、分散型ＤｏＳ攻撃者のホスト１１３、１１４、１１６、１１７からサーバ１０１への攻撃が終了すると、ルータ１０６、１０７、１０９、１１０にインストールされている移動型パケットフィルタリングのプログラムは、攻撃された履歴を前記境界ルータ１０２にインストールされている複製元の移動型パケットフィルタリングのプログラムに送信し、自分自身をルータ１０６、１０７、１０９、１１０から消去する。また本発明の移動型パケットフィルタリングのプログラムは、様々なネットワークの形態や通信内容に対して適用することが可能である。

【００３３】次に、図３および図４のフローチャートを参照しながら、移動型パケットフィルタリングの処理手順を説明する。この移動型パケットフィルタリングは、初期状態においては、防御対象のネットワークがその他のネットワークと接続されている接点に位置する境界ルータ（例えば、図１および図２に示すネットワークにおいてはルータ１０２）にインストールされている。

【００３４】この状態で、図３に示すステップＳ００１において、移動型パケットフィルタリングは、転送されてくるパケット（トラフィック）の監視を行っている。そして、Ｓ００２で監視結果がＤｏＳ攻撃であるか否かを判断する。この判断の結果として、ＤｏＳ攻撃が検出されなかった場合にはステップＳ００２からステップＳ００１へ戻る。つまり、ＤｏＳ攻撃が検出されないときはステップＳ００１の監視とステップＳ００２の判断を繰り返す。なお、ステップＳ００２においては、周知技術であるＤｏＳ攻撃の検出アルゴリズムを用いることによってＤｏＳ攻撃のデータのパターンを検出することができる。

【００３５】ステップＳ００２においてＤｏＳ攻撃が検出された場合には、ステップＳ００３に進み、ステップＳ００３において新しいプロセスを生成する。元のプロセスと新しく生成されるプロセスとは並行して処理を進めることができる。この元のプロセスは、ステップＳ００１に戻って受信トラフィックの監視を継続する。

【００３６】ステップＳ００３において新しく生成される第１のプロセスは、ステップＳ００４～Ｓ００６に記載されているように、当該ルータにおいて、検出した攻撃パケットを破棄する処理を行い、攻撃パケットが継続している間はパケットの破棄を継続する。攻撃パケットが停止した場合にはパケットの破棄処理を終了する。

【００３７】ステップＳ００３において新しく生成される第２のプロセスは、ステップＳ００７～Ｓ０１４に記載されている通り、上位のルータに防御位置を移動するための処理を行う。まず、ステップＳ００７においては、分散型ＤｏＳ攻撃か否かを判断する。なお、この分散型ＤｏＳ攻撃か否かの判断は周知技術によって行うことができる。この判断の結果、分散型ＤｏＳ攻撃でなかった場合にはそのまま処理を終了し、分散型ＤｏＳ攻撃であった場合には、図４のステップＳ００８に進む。

【００３８】ステップＳ００８においては、当該ルータが具備する隣接ルータデータベースを参照することにより、上位ルータとなり得るルータを検索する。ここで、上位ルータとなり得るルータとは、当該ルータに隣接するルータであって、かつ本発明が適用された移動型パケットフィルタリングの機能を果たすことのできるルータである。図２に示したネットワークを例にとると、境界ルータ１０２が具備する隣接ルータデータベースには、上位ルータとなり得るルータとして、ルータ１０３、１０４、１１１が格納されている。ルータ１０３および１０４は、境界ルータ１０２に隣接しているルータでありかつ本発明の移動型パケットフィルタリングの機能を果たすものである。また、ルータ１０５は本発明が適用さ

れてない通常ルータであるため、境界ルータ１０２からルータ１０５に向かう経路上のさらにひとつ先に存在しているルータ１１１が境界ルータ１０２の上位ルータとなる。すなわち、本発明の技術を装備するルータの中で、ネットワークトポロジーとして隣接しているルータの情報が隣接ルータデータベースに格納されている。

【００３９】ステップＳ００８での検索の結果をステップＳ００９において判断し、上位ルータが検索されなかった場合（ＮＯの場合）には、処理を終了する。また、上位ルータが検索された場合（ＹＥＳの場合）には、次のステップＳ０１０へ進む。図２に示した例では、境界ルータ１０２の隣接ルータとして上位ルータ１０３、１０４、１１１が検索されるため、Ｓ０１０の処理へ進む。

【００４０】ステップＳ０１０では、上で検出された上位ルータ１０３、１０４、１１１に対して、現在検索対象となっている分散型ＤｏＳ攻撃のパケットの情報を保持した攻撃元検索モジュールを送信する。

【００４１】ステップＳ０１１においては、上記の攻撃元検索モジュールを受信した上位ルータ上でこの攻撃元検索モジュールを実行することによって攻撃元検索モジュールが攻撃の防御に最適な位置を検索し、その結果が送信元の下位ルータに返送されてくる。なお、上記上位ルータのさらに上位ルータが存在する場合には、再帰的に攻撃元検索モジュールが送信され防御位置の検索が行われる。

【００４２】ステップＳ０１２においては、元のルータが上位ルータから検索結果を受信し、受信したアドレスの冗長情報を整理する。この冗長情報の整理については後で詳細に説明する。この冗長情報の整理が終了すると、ステップＳ０１３において、受信したアドレスが存在したか否かをチェックする。存在しなかった場合（ＮＯの場合）にはそのまま処理を終了し、存在した場合（ＹＥＳの場合）にはステップＳ０１４において冗長情報の整理後に残ったアドレスに対して攻撃防御モジュールを転送してから処理を終了する。

【００４３】次に、図４のステップＳ０１１で呼び出される攻撃元検索モジュールの処理内容について、図５および図６のフローチャートを参照しながら説明する。図５のステップＳ１０１において、送信された攻撃元検索モジュールが上位ルータへ到着する。図２に示したネットワークの例では、境界ルータ１０２から上位ルータ１０３、１０４、１１１にそれぞれこのモジュールが到着するが、ここでは、ルータ１０３へ到着したモジュールの実行を例として説明する。

【００４４】ステップＳ１０２では、攻撃元検索モジュールが保持している攻撃パケット情報を使い、ルータ１０３を攻撃パケットが通過しているか否かを検査し、その結果を送信元のルータへ報告する。ステップＳ１０３で検査結果をチェックし、攻撃パケットが通過していなかった場合（ＮＯの場合）にはそのままステップＳ１１２へ進む。攻撃パケットが通過していた場合（ＹＥＳの場合）には図６のステップＳ１０４へ進む。

【００４５】ステップＳ１０４においては、攻撃防御モジュールがインストール可能か否かを検査する。この検査は、例えば、当該ルータ上でのモジュール稼動のための各種資源が充分かどうかを調べるといった検査である。そして、ステップＳ１０５で上記検査結果を判断し、インストール可能な場合（ＹＥＳの場合）には、ステップＳ１１４で自分自身（ルータ１０３）のアドレスを最上位ルータアドレスの候補として保持して、ステップＳ１０６へ進む。インストール不可能な場合（ＮＯの場合）にはそのままステップＳ１０６へ進む。

【００４６】ステップＳ１０６では、自分自身（ルータ１０３）が具備する隣接ルータデータベースを参照して、上位ルータとなり得る隣接ルータを検索する。ルータ１０３にとっては、ルータ１０２、１０６、１０７、１０８が隣接ルータとして抽出される。

【００４７】そして、ステップＳ１０７では、上で抽出されたルータの中にさらなる上位ルータがあるか否かを検査する。ここでは、ルータ１０２は、攻撃元検索モジュールの送信元であるため、ルータ１０３のさらなる上位ルータではなく、ルータ１０６、１０７、１０８がさらなる上位ルータである。さらなる上位ルータがなかった場合（ＮＯの場合）には、Ｓ１０８に進み、保持している最上位ルータ候補を攻撃元検索モジュールの送信元へ送信する。さらなる上位ルータがあった場合（ＹＥＳの場合）には、ステップＳ１０９へ進む。

【００４８】ステップＳ１０９では、検出した全上位ルータに対して、ＤｏＳ攻撃の情報を保持した攻撃元検索モジュールを複製して送信し、全ての複製した攻撃元検索モジュールからの返事を待つ。

【００４９】ステップＳ１１０では、Ｓ１０９で送信された攻撃元検索モジュールを受信した上位ルータが当該モジュールを実行することにより最適防衛位置の検索の処理を行う。つまり、再帰的に上位ルータを検索することになる。

【００５０】ステップＳ１１１では、複製して送信した攻撃元検索モジュールからの返事を検査し、一個以上の検索モジュールからの返事に攻撃が通過しているという返事があった場合（ＹＥＳの場合）、そのままステップＳ１１２で自分自身を消滅させて処理を終了する。また、検索モジュールからの全ての返事が攻撃は通過していないという内容であった場合（ＮＯの場合）には、Ｓ１０８に進み、保持している最上位ルータ候補を攻撃元検索モジュールの送信元へ送信する。

【００５１】図４のステップＳ０１２で説明した検索結果のアドレスの冗長情報を整理する方法の詳細について説明する。図７は、アドレスの冗長情報を整理する手順を示す概略図である。前述した手順により、移動型パケ

ットフィルタリングプログラムは、識別された攻撃毎に最も攻撃元に近いルータを検出する。

【００５２】図７に示す表Ｔ００１は、検索の結果収集された情報を表している。この例の場合、同表の第１行目から第３行目までで表わされる各攻撃（攻撃元アドレスが「１１１．１１１．１１１．１１１」と「１１１．１１１．１１１．２２２」と「１１１．１１１．１１１．３３３」）については、攻撃元に一番近いルータ（アドレスが「１１１．１１１．１１１．１」）が同じになる可能性がある。このような冗長な情報は編集され、表Ｔ００２においてはひとつに集約される。そして、複製される移動型パケットフィルタリングプログラムは、表Ｔ００１から検出できる攻撃の数だけ複製されるのではなく、Ｔ００２から検出されたルータの数だけ複製され、同じ物を無駄に複製して同一の上位ルータに送らないようになっている。また、全ての複製された移動型パケットフィルタリングプログラムが、表Ｔ００２のような収集された情報全てを保持するのではなく、複製されて移動する先で移動型パケットフィルタリングが攻撃を防御するために利用する情報だけを取り出し、Ｔ００３に示すような効率の良い形式で保存される。

【００５３】次に、上述した複製された移動型パケットフィルタリングプログラムの処理手順について説明する。図８は、前記移動型パケットフィルタリングプログラムの処理手順を示すフローチャートである。以下、このフローチャートに沿って説明する。

【００５４】まず、ステップＳ０２１で、複製され攻撃の防御に必要な情報を受け取ると、当該プログラムは、インストールされるべきルータに向かって移動（送信）される。次に、ステップＳ０２２に進み、インストールされたルータで、攻撃元から攻撃先への全てのパケットを破棄する処理を行う。次に、ステップＳ０２３に進み、最後の攻撃が止まった時点からの時間を計測し、計測した時間が一定の時間に達する前に攻撃が再開されればステップＳ０２２に戻って防御を続け、計測した時間が一定の時間に達した場合には、ステップＳ０２４に進む。

【００５５】ステップＳ０２４では、攻撃に関する履歴情報（ログ）を複製元の移動型パケットフィルタリングプログラムへ送信する。最後にステップＳ０２５に進み、自分自身のプログラムをルータから消去し、処理を終了する。

【００５６】次に、上で説明した処理手順を実行するための構成について説明する。図９は、本実施形態によるルータの構成を示す構成図である。図示するように、このルータのハードウェア上ではオペレーティングシステム（ＯＳ）が稼動し、このオペレーティングシステム上で、本発明のモジュールが稼動する。なお、上記オペレーティングシステムは、システム全体の起動および終了を制御し、パケットフィルタリングの機能や、トラフィックスケジュール管理の機能や、ソケット機能や、ルーティングテーブル管理の機能や、中継パケット振り分け機能などを提供する。

【００５７】図１０は、本実施形態によって分散型ＤｏＳ攻撃を防止するための機能構成を示す構成図である。図示するように、本発明を実現する各機能は、ルータミドルウェア上の環境で動作する。なお、ルータミドルウェア環境は、前記オペレーティングシステムがバーチャルマシンとして提供する環境である。以下、図１０に示された各機能について個別に説明する。

【００５８】攻撃元判断機能部は、攻撃元検索モジュールが検索した攻撃元候補から攻撃防御モジュール（移動型パケットフィルタリングモジュール）を送り込むルータを抽出する機能を有する。この攻撃元判断機能部は、図４に示したステップＳ０１２の処理を行う。

【００５９】攻撃元検索モジュールは、攻撃元に最も近いルータのアドレスを検索するために、他のルータに送り込まれるプログラムモジュールである。この攻撃元検索モジュールは、図５および図６に示した処理を行う。

【００６０】攻撃防御モジュール（移動型パケットフィルタリングモジュール）は、攻撃を止めるために攻撃元に近いルータに送り込まれるプログラムモジュールである。この攻撃防御モジュールは、図８に示した処理を行う。

【００６１】攻撃元ルータ情報受信部は、上位ルータ上で稼動する攻撃元検索モジュールから検索結果の攻撃元ルータの情報を受信する機能を有する。この攻撃元ルータの情報は、図６のステップＳ１１４の処理において上位側のルータから送信されてくる情報である。

【００６２】攻撃元アドレス管理部は、上記攻撃元ルータ情報受信部が攻撃元検索モジュールから受信したアドレス、つまり攻撃防御モジュールの送信先ルータのアドレスを保存し管理する機能を有する。

【００６３】攻撃情報管理部は、分散型ＤｏＳ攻撃の情報を管理する機能である。

【００６４】トラフィック監視機能部は、ルータを通過するトラフィックを監視し、分散型ＤｏＳ攻撃を検出する機能を有する。このトラフィック監視機能部は、図３に示したステップＳ００２およびＳ００７の判断を行う。

【００６５】モジュール複製機能部は、攻撃元検索モジュールや攻撃防御モジュールを複製する機能を有する。

【００６６】隣接ルータデータベースは、本発明の技術を適用したルータであってネットワークトポロジーの上で当該ルータに隣接するルータの情報を格納するデータベースである。

【００６７】攻撃元ルータ情報受信部は、上位ルータ上で稼動する攻撃元検索モジュールから検索結果の攻撃元ルータの情報を受信する機能を有する。

【００６８】モジュール送信部は、攻撃元検索モジュー

ルや攻撃防御モジュールを他のルータへ送信する機能を有する。

【００６９】攻撃防御機能部は、攻撃パケットを破棄する機能を有する。

【００７０】攻撃元アドレス整理部は、上位のルータから受信した最適防衛位置に関するアドレス情報を整理する機能を有する。つまり、この攻撃元アドレス整理部が、図７に示したようにアドレスの冗長性を整理する処理を行う。

【００７１】図１１は、攻撃元検索モジュールのさらに詳細な構成を示す構成図である。図示するように、攻撃元検索モジュールは、隣接ルータ検査機能部と、トラフィック検査機能部と、攻撃通知機能部と、自己消滅機能部の各機能部を備え、攻撃パケット情報と最上位ルータ候補の情報を保持することができる。

【００７２】隣接ルータ検査機能部は、ルータが具備する隣接ルータデータベースから、上位ルータとしての検査対象を抽出する機能を有する。

【００７３】トラフィック検査機能部は、ルータを通過中のトラフィックと攻撃パケット情報とを比較して、攻撃パケットがルータを通過中であることを検知した場合には、上位ルータを最上位ルータ候補として記録する機能を有する。

【００７４】攻撃通知機能部は、攻撃元の検索を終わった後に複製元の攻撃検索モジュールへ最上位ルータ候補のアドレスを通知する機能と、攻撃元の検索中に攻撃が行われていなかった場合には攻撃が行われていない旨を通知する機能を有する。

【００７５】自己消滅機能部は、攻撃元検索モジュールが不必要になった時点で攻撃元検索モジュール自身をルータ上から消去する機能を有する。

【００７６】攻撃パケット情報は、分散型ＤｏＳ攻撃の攻撃元候補の一つを保持している。また、最上位ルータ候補は、攻撃元の最上位ルータの候補の情報を保持している。

【００７７】図１２は、攻撃防御モジュールのさらに詳細な構成を示す構成図である。図示するように、攻撃防御モジュールは、攻撃防御機能部と、攻撃トラフィック監視機能部と、自己消滅機能部の各機能部を備え、攻撃パケット情報を保持することができる。

【００７８】攻撃防御機能部は、攻撃パケットを破棄する機能を有する。攻撃トラフィック監視機能部は、攻撃が継続中か否かを監視する。自己消滅機能部は、攻撃が中断した場合には攻撃防御モジュール自身をルータ上から消滅させる機能を有する。

【００７９】以上、本実施形態の理解を助けるために要約すると、パケットフィルタリングを行う装置が一つのルータやルータ設置箇所に限定されず、前記パケットフィルタリングのプログラムは、分散型ＤｏＳ攻撃を防ぐのに最適な位置に存在するルータに移動する。この移動先になる最適な位置を検出するために、パケットフィルタリングのプログラムは、公知技術であるＣｅｎｔｅｒＴｒａｃｋなどの既存の追跡技術を利用し、分散型ＤｏＳ攻撃の攻撃元に向かって自分自身のプログラムを移動させる。

【００８０】本発明では、パケットフィルタリングのプログラムの複製を作成し、その複製を様々な位置に存在するルータに移動させることもできる仕組みも含まれる。この仕組みは、複数箇所から同時に攻撃してくる分散型ＤｏＳ攻撃の各攻撃元でパケットフィルタリングを動作させることによって、分散型ＤｏＳ攻撃を防御することに利用する。本発明に基づくシステムでは、パケットフィルタリング機能は、最初は防御対象であるローカルエリアネットワークがインターネットに接続される境界に存在するルータにインストールされ、分散型ＤｏＳ攻撃を検知した時に、分散型ＤｏＳ攻撃の複数の攻撃元各々に近いルータに複製を移動させる。移動先は、できるだけ攻撃元に近いルータを目指すため、攻撃元の端末が接続されているローカルエリアネットワークがインターネットに接続されている境界に存在するルータが一番効果的ではあるが、必ずしもその境界に存在するルータである必要はない。

【００８１】また、複製されたパケットフィルタリング機能には、自分自身の移動履歴、フィルタリングしたパケットの履歴を保存し、それを複製元に送信する機能を有する。

【００８２】さらに、複製されたパケットフィルタリング機能には、自分自身を消去する機能も有する。これは、複製されたパケットフィルタリングが防御していた攻撃が終了してからある一定の時間が過ぎた場合にルータから自分自身の機能を消去するという動作や、複製されたパケットフィルタリングがインストールされているルータの方針によって消去されるという動作になる。

【００８３】以上、本実施形態によれば、送信元アドレスを詐称したパケットによる分散型ＤｏＳ攻撃を防御する際に、送信元アドレスの詐称の如何に関わらず、攻撃を防御できる分散サービス不能攻撃の防止方法および装置を提供できる。

【００８４】＜第２の実施形態＞次に、本発明の第２の実施形態について説明する。前記の第１の実施形態は攻撃元検索モジュールが全ての攻撃情報を保持して移動する形態であったが、この第２の実施形態では、攻撃元検索モジュールはひとつの攻撃元情報だけを保持して移動するという特徴がある。

【００８５】図１３および図１４は、本実施形態による移動型パケットフィルタリングの処理の手順を示すフローチャートである。以下、このフローチャートに沿って説明する。

【００８６】図１３のステップＳ２０１からＳ２０３までの処理は、図３に示したステップＳ００１からＳ００

３までの処理と同様である。また、ステップＳ２０４からＳ２０６までの処理およびステップＳ２０７の処理も、図３に示したステップＳ００４からＳ００６までの処理およびステップＳ００７の処理とそれぞれ同様である。

【００８７】図１４のステップＳ２０８からＳ２０９までの処理は、図４に示したステップＳ００８からＳ００９までの処理と同様である。ステップＳ２１０では、攻撃元アドレス管理部から新たな攻撃元のアドレスを１つ抽出する。そして、ステップＳ２１１において、全てのアドレスの処理を終了したと判断した場合は、全体の処理を終了する。また、ステップＳ２１２からＳ２１６までにおいては、ステップＳ２１０で抽出した攻撃元アドレスに関して、図４に示したステップＳ０１０からＳ０１４までと同様の処理を実行する。そして、ステップＳ２１０に戻って次の攻撃元アドレスの処理を抽出する。

【００８８】なお、この第２の実施形態において、上位ルータに対して送信される攻撃元検索モジュールと攻撃防御モジュールの処理の手順は、前述の第１の実施形態におけるそれらと同様のものである。

【００８９】＜第３の実施形態＞次に、本発明の第３の実施形態について説明する。前記の第１および第２の実施形態は、攻撃元検索モジュールと攻撃防御モジュールとが別個のモジュールであったが、この第３の実施形態では、攻撃元検索モジュールの機能と攻撃防御モジュールの機能とが一体となったモジュール（以下では、便宜上「攻撃防御モジュールＢ」と呼ぶ）を用いるという特徴がある。

【００９０】図１５および図１６は、本実施形態による移動型パケットフィルタリングの処理の手順を示すフローチャートである。以下、このフローチャートに沿って説明する。

【００９１】図１５のステップＳ３０１からＳ３０３までの処理は、図３に示したステップＳ００１からＳ００３までの処理と同様である。また、ステップＳ３０４からＳ３０６までの処理およびステップＳ３０７の処理も、図３に示したステップＳ００４からＳ００６までの処理およびステップＳ００７の処理とそれぞれ同様である。

【００９２】図１６のステップＳ３０８からＳ３０９までの処理は、図４に示したステップＳ００８からＳ００９までの処理と同様である。ステップＳ３１０では、ステップＳ３０９で得られた全ての上位ルータに対して、攻撃パケットの情報を保持した前記攻撃防御モジュールＢを送信する。そして、ステップＳ３１１においては、送信先の上位ルータにおいて前記攻撃防御モジュールＢの処理が実行される。つまり、上位ルータにおいて攻撃防御が行われるとともに、さらに上位のルータの検索が行われ、再帰的にさらに上位のルータに対して当該モジュールが送信される。

【００９３】図１７は、本実施形態による攻撃防御モジュールＢの処理の手順を示すフローチャートである。以下、このフローチャートに沿って説明する。

【００９４】図１７のステップＳ４０１において、送信された攻撃防御モジュールＢが上位ルータへ到着する。ステップＳ４０２では、攻撃防御モジュールＢが保持している攻撃パケット情報を使い、当該ルータを攻撃パケットが通過しているか否かを検査し、その検査結果に応じて、通過していた場合にはステップＳ４０３へ進み、通過していなかった場合にはステップＳ４１１で攻撃防御モジュールＢ自身を当該ルータから消滅させて処理を終了する。

【００９５】ステップＳ４０３では、新しいプロセスを生成し、攻撃パケットの破棄と上位ルータの検索とを並行して行えるようにする。

【００９６】ステップＳ４０３において分岐（fork）した第１のプロセスは、ステップＳ４０４からＳ４０６までにおいて、攻撃が停止されるまで攻撃パケットを破棄し、自プロセスを消滅させて処理を終了する。なお、ステップＳ４０４からＳ４０６までの処理は、図３に示したステップＳ００４からＳ００６までの処理と同様である。

【００９７】ステップＳ４０３において分岐（fork）した第２のプロセスは、ステップＳ４０７からＳ４１０までの処理を行う。なお、ステップＳ４０７からＳ４１０までの処理は、図１６に示したステップＳ３０８からＳ３１１までの処理と同様である。その後、ステップＳ４１１において自プロセスを消滅させて処理を終了する。

【００９８】つまり、攻撃防御モジュールＢは、再帰的に上位ルータを検索し、その上位ルータに対して攻撃防御モジュールＢ自身を送信し、送信先の上位ルータにおいてさらに攻撃防御モジュールＢの処理が実行される。そして、攻撃元に最も近い最上位ルータにおいてこの再帰が停止し、この最上位ルータでは攻撃が停止されるまで攻撃パケットの破棄が続けられることとなる。

【００９９】図１８は、攻撃元を検索する機能と攻撃を防御する機能の両方を有する前記攻撃防御モジュールＢの構成を示す構成図である。図示するように、攻撃防御モジュールＢは、隣接ルータ検査機能部と、トラフィック検査機能部と、攻撃防御機能部と、攻撃トラフィック監視機能部と、自己消滅機能部の各機能部を備え、攻撃パケット情報を記憶できるようになっている。

【０１００】これらのうち、隣接ルータ検査機能部と、トラフィック検査機能部と、自己消滅機能部とは、第１の実施形態における攻撃元検索モジュールの構成として図１１に示した同一名称の各機能部と同様のものである。また、攻撃防御機能部は、同じく図１２に示した攻撃防御機能部と同様のものである。

【０１０１】＜ネットワークの中継ノード（ルータ）上での各種機能の実行方法＞前記第１から第３までの実施

形態においては、ルータからルータへプログラムモジュールを転送し、受信側のルータでそのプログラムモジュールを実行し、中継ノードを通過する通信データに対する処理を行うことができることを前提としていた。ここでは、そのようなプログラムモジュールの転送および実行の方法について説明する。

【０１０２】近年、インターネットの利用が様々な方面に拡大するにしたがって、ネットワークノードがパケットを転送するだけでは、利用者の様々なニーズに応えることは既にできなくなってきている。また、各種のネットワーク機器製造者は、例えばマルチキャストやＲＳＶＰ（Resource Reservation Protocol）といった新しいサービスを、ネットワーク機器のファームウェアをアップグレードすることによって実現してきた。

【０１０３】一方、アクティブネットワーク技術とよばれるものは、ネットワークの中継ノードにプログラムの実行環境を提供することと、その実行環境の上で標準化された機能モジュールを実行させることによって、新しいネットワークサービスを迅速に開発できるようにすることを目標としている。従来のネットワークでは、通信端末はＩＰパケットの送信元、あるいは送信先アドレス以外には、ほとんどオプションを指定することはできないが、このアクティブネットワークでは、送信元の通信端末から送出されたパケットが、送信先の通信端末に到達する前にどのような処理をするのかという指定ができる。アクティブネットワークの方式は以下の３点に分けられる。

【０１０４】第１にアクティブパケット方式がある。このアクティブパケット方式は、パケットに小規模なプログラムを埋め込む方式である。このプログラムは、中継ノードにて取り出され実行される。第２は、アクティブノード方式である。このアクティブノード方式は、中継ノードにプログラムを事前にインストールしておく方法である。事前に定義したサービスを識別するＩＤをパケットに付加することによって、中継ノードで実行されるプログラムを指定する。第３のアクティブパケット・ノードは、前記第１と第２の方式を組み合わせた方式で、両者の利点が組み合わさっている。これら３種類の方式は、ＡＮＥＰ（Active Network Encapsulation Protocol）ヘッダのような新しいヘッダ方式を利用することが求められる。

【０１０５】上述した、マルチキャストやＲＳＶＰといった新しいサービスは、ネットワーク機器のファームウェアをアップグレードすることによって実現してきたが、この方法には、コストがかさむ上にサービス開発に期間を要する、さらに、異なるハードウェア毎にソフトウェアを開発しなければならない、といった問題点がある。

【０１０６】また、上述のアクティブネットワークの３方式は、いずれもデータを送信する端末からパケットが送出される前に、パケットにプログラムを埋め込む、または予め定義したサービスＩＤを付加するなど、従来のＩＰパケットには無かった送信データに対して処理を行う指示を与えるための情報を付加することが必要である。これらを実現するためには、データを送出する端末のアプリケーション、またはＩＰパケットの処理プログラムなどで、情報をパケットに付加する処理を行う。このため、通信端末上のアプリケーションやＩＰパケットの処理プログラムを変更しなければならないという問題があり、コスト的にも負担が強いられるものであった。

【０１０７】本発明においては、中継ノードの機種に制限されることなくサービスモジュールが移動することができるようになり、また、中継ノードにインストールされているサービスモジュールを利用するために、コンピュータなどの通信端末にインストールされているソフトウェアを変更する必要がなくない、ネットワーク通信機器でプログラムを動作させることができるように、以下に述べるような手段を提供している。

【０１０８】すなわち、この発明で用いるのネットワーク通信機器でプログラムを動作させる方法及び装置は、ネットワークに配置された中継ノードに動的にプログラムをインストールするためのプラットフォーム手段と、前記インストールされたプログラムに対してアプリケーションインターフェイスを提供する手段と、前記プログラムが動作する際には、前記中継ノードに送られてきたパケットが前記プログラムの処理対象であればプログラムに対してパケットを引き渡す手段と、前記処理が終わった後にパケットを送出する手段とを具備する。

【０１０９】このネットワーク通信機器でプログラムを動作させる技術について、図面を用いてさらに詳細な実施方法を用いて説明する。

【０１１０】図１９は、システムの概略構成を示す構成図である。図１９に示すように、通信端末１と７が、通信ネットワーク５にて接続されており、ルータ、ＡＴＭ（Asynchronous Transfer Mode）スイッチおよびＩＰパケットを転送する能力を持つコンピュータの３種類の機能を統合して備えているネットワークの中継ノード２、４および６によって接続されている。モジュールサーバ３は、サービスモジュールの開発者（図示せず）から送られてくる新しいモジュールを受信し、このモジュールと一緒に送られてくる電子署名によって開発者の認証を行う。このようにコンピュータシステムが使うハードウェアシステムとシステムソフトウェア（プラットフォーム）が配置されている。

【０１１１】次に、図２０は、上述したモジュールサーバ３の構成を示す構成図である。サービスモジュール受信部１１は、あらかじめ登録されている認定開発者のデータベース１２の情報を使い、受信したサービスモジュールに付加されている電子署名を検査することによって、開発者の認証を行う。その後に、サービスモジュー

ル受信部１１は、受信したサービスモジュールが、インターフェイスとセキュリティの要求条件を満たしていることを検査する。そして、検査が済んだモジュールは、サービスモジュールデータベース１３に保存される。この保存されたサービスモジュールの名称およびサービス概要は、サービスメニュー１４に表示されるようになる。このプライベートサービスメニュー１４は、ネットワークの利用者がネットワーク経由で見ることができ、エンドユーザはメニューの内容を見てサービスを要求する。要求を受け取るとユーザデータベース１７の内容を検査し、要求を送信してきたネットワーク利用者が要求する権限があることが確認されると、サービスモジュールインジェクタ１５は、ネットワーク利用者から要求されたサービスモジュールをネットワーク中継ノードに転送する。このとき、サービスマネージャ１６は、サービスモジュールを転送した先を記録し、その後にサービスモジュールが他の中継ノードに移動した場合は移動先の情報をサービスモジュールから受け取り、サービスモジュールが動作中かといった状態の情報もサービスモジュールから受け取り管理する。

【０１１２】次に、図２１は、本発明を実装したネットワーク中継ノード（ルータ）の概要を表しており、また図２２は、前記中継ノード内のノードカーネルおよび実行エンジンの機能を示す表図である。なお、このノードカーネルと実行エンジンとは、図９に示したＯＳを構成する機能である。

【０１１３】図２１に示すように、ノードカーネル２０は、前記中継ノードに実装された本システムの起動／終了、また、中継ノードに実装されている機器と本システムとの入出力管理、パケットフィルタリングやトラフィックデータのスケジュール管理やソケット処理やルーティングテーブルの操作といった中継ノードのメーカ毎に異なる処理に対するインターフェイスを提供し、実行エンジン２１やサービスモジュール２２は、前記ノードカーネル２０に対してパケットフィルタリングなどの処理を要求すると、このノードカーネル２０がその処理を仲介する。さらに、ノードカーネル２０は、ＩＰパケットが中継ノードに転送されてきた時に、この中継ノードにインストールされているサービスモジュール２２が処理するべきパケットであれば、実行エンジン２１を経由してサービスモジュール２２にパケットを振り分ける。一方、前記中継ノードにインストールされているサービスモジュール２２が処理するべきパケットでなければ、そのまま通常のＩＰパケットとして処理し転送する。このときのどのパケットを処理するかという情報は、モジュールサーバ３（図１９参照）からサービスモジュール２２と共に送られてくる。

【０１１４】また、実行エンジン２１は、新規のサービスモジュール２２がモジュールサーバ３から送られていることを常時待機しており、サービスモジュール２２の

処理を開始すると処理の状態を監視し、必要に応じてその状態の情報を前記モジュールサーバ３に送信する。

【０１１５】次に、図２３は、前記中継ノードが受信したパケットを、本発明に基づいてどのように処理するのかを表したフローチャートである。まず、ステップＳ１００１で、ある中継ノードが隣接する中継ノードなどからＩＰパケットを受信する。次に、Ｓ１００２に進み、この受信したパケットの送信元アドレスまたは送信先アドレスが、前記中継ノードにインストールされているサービスモジュールのいずれかが処理すべき対象になっているか否かを調べる。送信元アドレスまたは送信先アドレスがサービスモジュールの処理すべき対象アドレスとして指定されている場合は、Ｓ１００３に進み、処理すべき対象として指定しているサービスモジュール２２（図２１参照）にパケットを引渡し、前記サービスモジュール２２が処理を行う。また、処理すべき対象となっていないパケットの場合は、Ｓ１００４に進み、通常のＩＰパケットとして、送信先アドレスにＩＰパケットが到達するように、ルーティングテーブルなどを参照して転送処理を行う。なお、前記Ｓ１００２の判断条件は、ＩＰパケットの送信先または送信元アドレスという態様を示したが、その条件だけに限らず、サービスモジュール２２が条件を自由に設定することができる。

【０１１６】次に、図２４は、前記サービスモジュール２２（図２１参照）をモジュールサーバ３（図１９参照）に送信する手順を示しているフローチャートである。まずＳ１０１１では、前記サービスモジュール２２の開発者からサービスモジュール２２の送信要求と共にサービスモジュール２２のプログラム、開発者の電子署名を受信する。次に、Ｓ１０１２に進み、前記電子署名の有無を検査し、付加されている場合はさらにＳ１０１３に進み、前記開発者が事前に登録されているか否かを検査し、登録されている場合はＳ１０１４に進み、前記サービスモジュール２２のプログラムが要求条件を満たしているか否かの検査を行う。また、Ｓ１０１２，Ｓ１０１３およびＳ１０１４の条件は、どれか一つでもが満たされない場合には、Ｓ１０１５に進み、サービスモジュール２２の受信を拒否し処理を終了する。全ての条件が満たされた場合は、Ｓ１０１６に進み、サービスモジュール２２をデータベースに登録し、サービスメニューの内容を更新する。

【０１１７】次に、図２５は、ネットワーク利用者からサービスモジュールの要求を受信する手順を示したフローチャートである。まずＳ１０２１では、前記ネットワーク利用者からのサービスモジュール２２（図２１参照）の要求を受信する。そして、Ｓ１０２２に進み、前記要求と共に送られてきたネットワーク利用者の情報から、要求を送信してきたネットワーク利用者が正規の利用者であることを確認する。もし正規の利用者であれば、Ｓ１０２３に進み、前記ネットワーク利用者から受

信した要求に含まれるサービスモジュール２２がモジュールサーバ３（図１９参照）に保存されているか、ネットワーク利用者が要求できる権限を持っているサービスモジュール２２なのかといったネットワーク利用者の要求したサービスモジュール２２に対する正当性の検査を行う。前記Ｓ１０２２またはＳ１０２３でいずれか一方の条件が満たされない場合、Ｓ１０２４に進みエラーメッセージを表示して処理を終了する。

【０１１８】次にＳ１０２５に進み、前記ネットワーク利用者の情報をモジュールサーバ３に保存されているユーザデータベースから収集する。続いてＳ１０２６に進み、前記利用者の情報に含まれるサービスモジュール２２を要求してきたネットワーク利用者の接続しているネットワークに関する情報から、要求されたサービスモジュール２２が処理できるパケットを定義する。さらに、Ｓ１０２７に進み、前記Ｓ１０２５で収集したサービスモジュール２２を要求してきたネットワーク利用者が接続するネットワークに関する情報から、前記ネットワークがインターネットに接続している境界に存在する中継ノードを導き出し、その導き出した境界に存在する中継ノードにサービスモジュール２２を転送して、終了する。

【０１１９】次に、図２６は、サービスモジュール２２の論理構造を示している。プライベートサービスモジュールの行動を管理するために、ここでは、中継ノードにサービスモジュール２２をインストールする前に７種類の属性を付加する。この７種類の属性とは、サービスＩＤ、オーナＩＤ、インストール時間、開発者ＩＤ、モジュールサーバＩＰアドレス、複製情報、処理対象である。前記複製情報と処理対象は、以下で詳しく説明する。

【０１２０】前記サービスモジュールは、元々インストールされている中継ノードから移動することができ、場合によっては、前記サービスモジュールが複製を作成して複数の中継ノードで処理を行うことも可能である。このように複製したサービスモジュールを見分けるために、モジュールサーバから中継ノードにインストールされたサービスモジュールをオリジナルとし、このインストールされたサービスモジュール以外の複製が他の中継ノードに作成されたときには、複製されたサービスモジュールとし、それぞれを区別する情報を複製情報としてサービスモジュールは保持する。この処理対象は、ネットワーク利用者がモジュールサーバに、サービスモジュールを要求した時点で生成される。また、前記モジュールサーバは、ユーザ情報のデータベースを調べ、サービスモジュールが処理対象として良いパケットをＩＰアドレスなどによって決定する。そして、処理対象として許可するのは、サービスモジュールを要求したエンドユーザが送信元または送信先になっているデータであり、ＩＰアドレス以外の情報を用いて識別することもできる。

【０１２１】前記ネットワーク利用者は、サービスモジュールをメニューから選んで要求する。この際に、要求するサービスモジュールを指定するサービスＩＤの他に、前記サービスモジュールの初期状態を指定するパラメータも同時にモジュールサーバに送信することができる。この場合、初期設定が終了すると、サービスモジュールは中継ノードにインストールされる。このインストールされる中継ノードは、特に指定が無い場合は、前記サービスモジュールを要求したネットワーク利用者が属しているネットワークに一番近いノードになる。そして、前記サービスモジュールは、中継ノードにインストールされると、他の条件を待たずに、パケットの処理、他の中継ノードへの移動、複製の作成などを開始できるが、どのような処理を行うのかは、サービスモジュールにサービスモジュールの開発者がプログラムしてあるアルゴリズムとネットワーク利用者が初期値として指定したパラメータに依存する。

【０１２２】前記サービスモジュールには、セキュリティの観点から実行に関する以下の制限を加える。第１は、使用制限である。この使用制限は、ある特定の時点で使用できるサービスの数であり、サービスモジュールは処理を終了すると直ちに中継ノードから消え去るようにもできる。また、利用中のサービスモジュールの数が制限に達すると、それ以上は新規のサービスを実行することはできず、モジュールサーバ内のサービスモジュールマネージャが、全てのユーザの使用中のサービス数を監視するものである。

【０１２３】第２は、複製モジュールである。この複製モジュールは、複製元のモジュールが存在しなくなると、自動的に存在できなくなる。そして、複製元のモジュールが無くなると、モジュールサーバによって複製モジュールも消去される。また、複製モジュールが一定時間以上パケットの処理を行わないと、実行エンジンによって消去される。すなわち、複製モジュールが処理を続けるためには、パケットを受信しつづける必要がある。

【０１２４】第３は、サービスモジュールである。このサービスモジュールは、自分自身に設定されている終了条件に達したとき、またはそのサービスモジュールを要求したネットワーク利用者がモジュールサーバを経由して明示的に終了の指示を伝えてきたときにだけ終了する。この条件は全てのサービスモジュールに適用される。

【０１２５】第４は、処理対象パケットである。サービスモジュールが処理できるパケットには制限があり、前記サービスモジュールは、そのサービスモジュールを要求したネットワーク利用者が属するネットワークに所属する通信端末が送信元、あるいは送信先になっているデータしか処理をすることができないことによる。

【０１２６】第５は、処理対象の競合である。上記第４で述べたようにサービスモジュールが処理できるパケッ

トには制限があるが、あるパケットに着目すると、必ず送信元の利用者と送信先の利用者がいることになる。このため、ある中継ノードで、転送されてきたＩＰパケットの送信元および送信先の両者のネットワーク利用者からサービスモジュールがインストールされていることがありうる。このときは、送信先のサービスモジュールだけがパケットに対して処理をできる権限を与える。

【０１２７】第６は、モジュールの競合である。ある中継ノードに同じネットワーク利用者から複数のサービスモジュールがインストールされている場合、最初にインストールされたサービスモジュールだけがＩＰパケットに対して処理を行うことができる。

【０１２８】第７は、パケットの入出力である。前記サービスモジュールは、それ自身が新しいＩＰパケットを生成することはできない。すなわち、転送されてきたパケット一つに対して、転送するパケットも一つになる。

【０１２９】第８は、ロケーション管理である。前記サービスモジュールは複製モジュールも含めて全て中継ノード間を移動することができるため、移動する場合には、新しい中継ノードの場所もモジュールサーバ内のモジュールマネージャに通知する。このように、前記サービスモジュールには、セキュリティの観点から実行に関する制限を加えている。

【０１３０】以上、説明した技術を用いることによって、製造業者が異なる中継ノードで仕様の異なるプログラムインターフェイスを統一した形でサービスモジュールへ提供する実行環境を提供することになり、サービスモジュールがインストールできる中継ノードであれば、その機種に制限されることなくサービスモジュールが移動することができるようになる。また、従来のＩＰパケットのままでサービスモジュールの処理対象を特定する方法によって、アクティブネットワークなどの従来技術ではパケット自体を改変する必要があったものを不要とした。これによって、中継ノードにインストールされているサービスモジュールを利用するために、コンピュータなどの通信端末にインストールされているソフトウェアを変更する必要がなくなる。

【０１３１】なお、上述した各コンピュータプログラムは、コンピュータ読取可能な記録媒体に記録されており、通信装置等に搭載されたＣＰＵ（中央処理装置）がこの記録媒体からコンピュータプログラムを読み取って、攻撃防御あるいはサービスモジュール提供等のためも各処理を実行する。また、「コンピュータ読み取り可能な記録媒体」とは、磁気ディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。

【０１３２】また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されても良い。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

【０１３３】また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムに既に記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【０１３４】以上、図面を参照してこの発明の実施形態を詳述してきたが、具体的な構成はこれらの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【０１３５】

【発明の効果】以上説明したように、本発明によれば、通信装置が、分散型サービス不能攻撃を防止するための通信装置であって、当該通信装置を通過する通信パケットを監視し分散型サービス不能攻撃を検出するトラフィック監視機能部と、分散型サービス不能攻撃が検出された際に当該分散型サービス不能攻撃の通信パケットを破棄する攻撃防御モジュールと、攻撃元に近い上位側の通信装置のアドレスを検索する処理を行う攻撃元検索モジュールと、上位側の防御位置の通信装置に対して前記攻撃元検索モジュールを送信するモジュール送信部と、前記攻撃元検索モジュールによって検索された攻撃元に近い上位側の通信装置の候補中から上位側の防御位置とする通信装置を抽出する攻撃元判断機能部とを備え、前記モジュール送信部は、前記攻撃元判断機能部によって抽出された上位側の防御位置の通信装置に対して前記攻撃防御モジュールを送信するため、分散型サービス不能攻撃を検出した際には、検出した通信装置において攻撃の通信パケットを破棄するとともに、より攻撃元に近い上位の通信装置を検索し、その検索の結果得られた上位の通信装置に対して攻撃元検索モジュールを送信し、この上位の通信装置においてこのモジュールを実行することによって当該上位のモジュールを当該攻撃の通信パケットが通過しているかどうかを判断し、通過している場合には、再帰的にさらに上位の通信装置を検索していくことができるので、攻撃元に最も近い最上位の通信装置において攻撃を防御する、すなわち攻撃の通信パケットを破棄することが可能となる。これにより、攻撃の通信パケットによる影響を攻撃元に近い局所に限定することが可能となり、ネットワーク全体への悪影響を抑制することができる。

【０１３６】また、例えばインターネットのように、本来攻撃防御の機能を備えていないネットワークであっても、本発明を適用することによって攻撃に対する効果的な防御が可能になる。また本発明を用いた場合、攻撃者が直接接続されているネットワークの管理者が何らかの対処をする必要がなく、攻撃を受けている装置が接続されているネットワーク側の対処によって自動的に防御機能が起動され攻撃を防ぐことができるようになる。

【０１３７】また本発明によれば、通信装置が、当該通信装置を通過する通信パケットを監視し分散型サービス不能攻撃を検出するトラフィック監視機能部と、分散型サービス不能攻撃が検出された際に当該分散型サービス不能攻撃の通信パケットを破棄するとともに、攻撃元に近い上位側の通信装置のアドレスを検索する処理を行う攻撃防御モジュールと、上位側の通信装置に対して前記攻撃防御モジュールを送信するモジュール送信部とを備えるため、攻撃元を検索する機能と攻撃を防御する機能とを単一のプログラムモジュールで実現できるとともに、防御のアルゴリズムを単純化することが可能となる。

【０１３８】また、本発明によれば、通信装置に対してプログラムモジュールを送信するモジュールサーバが、前記通信装置にインストールされるプログラムモジュールを保存するプログラムモジュールデータベースと、前記プログラムモジュールの保存を依頼できるプログラムモジュールの開発者を管理する開発者データベースと、前記プログラムモジュールを前記通信装置にインストールする要求ができる利用者を管理するユーザデータベースと、保存されている前記プログラムモジュールを前記利用者にメニューで表示するサービスメニューと、前記サービスメニューに表示されている前記プログラムモジュールをインストールする要求が前記利用者からあれば前記利用者の権限を認証するサービスマネージャと、前記認証を確認できた場合には前記プログラムモジュールを前記通信装置に対して送信するサービスモジュールインジェクタとを備えるモジュールサーバを備えることによって、所定の開発者によって開発されたプログラムモジュールだけが通信装置上で実行可能となり、通信システムの信頼性がより一層向上する。

【図面の簡単な説明】

【図１】　本発明を適用できるネットワークの構成図である。

【図２】　図１に示したネットワークにおいて行われている分散型ＤｏＳ攻撃に対する防御方法を示す概略図である。

【図３】　本発明の第１の実施形態による移動型パケットフィルタリングの処理手順を示すフローチャートの一部分である。

【図４】　本発明の第１の実施形態による移動型パケットフィルタリングの処理手順を示すフローチャートの一部分である。

【図５】　本発明の第１の実施形態による攻撃元検索モジュールの処理の手順を示すフローチャートの一部分である。

【図６】　本発明の第１の実施形態による攻撃元検索モジュールの処理の手順を示すフローチャートの一部分である。

【図７】　本発明の第１の実施形態により攻撃元に近い上位ルータのアドレスの冗長情報を整理する手順を示す概略図である。

【図８】　本発明の第１の実施形態による移動型パケットフィルタリングプログラムの処理手順を示すフローチャートである。

【図９】　本発明の第１の実施形態によるルータの構成を示す構成図である。

【図１０】　本発明の第１の実施形態によって分散型ＤｏＳ攻撃を防止するための機能構成を示す構成図である。

【図１１】　本発明の第１の実施形態による攻撃元検索モジュールの詳細な構成を示す構成図である。

【図１２】　本発明の第１の実施形態による攻撃防御モジュールの詳細な構成を示す構成図である。

【図１３】　本発明の第２の実施形態による移動型パケットフィルタリングの処理の手順を示すフローチャートの一部分である。

【図１４】　本発明の第２の実施形態による移動型パケットフィルタリングの処理の手順を示すフローチャートの一部分である。

【図１５】　本発明の第３の実施形態による移動型パケットフィルタリングの処理の手順を示すフローチャートの一部分である。

【図１６】　本発明の第３の実施形態による移動型パケットフィルタリングの処理の手順を示すフローチャートの一部分である。

【図１７】　本発明の第３の実施形態による攻撃防御モジュールＢの処理の手順を示すフローチャートである。

【図１８】　本発明の第３の実施形態による攻撃防御モジュールＢの構成を示す構成図である。

【図１９】　本発明の適用対象であるネットワーク通信機器上でプログラムを動作させるためのシステムの概略構成を示す構成図である。

【図２０】　モジュールサーバの構成を示す構成図である。

【図２１】　ネットワーク中継ノード（ルータ）の概要を表す概略図である。

【図２２】　中継ノード内のノードカーネルおよび実行エンジンの機能を示す表図である。

【図２３】　前記中継ノードが受信したパケットを処理する手順を示すフローチャートである。

【図２４】　サービスモジュールをモジュールサーバに

送信する手順を示すフローチャートである。

【図２５】　ネットワーク利用者からサービスモジュールの要求を受信する手順を示すフローチャートである。

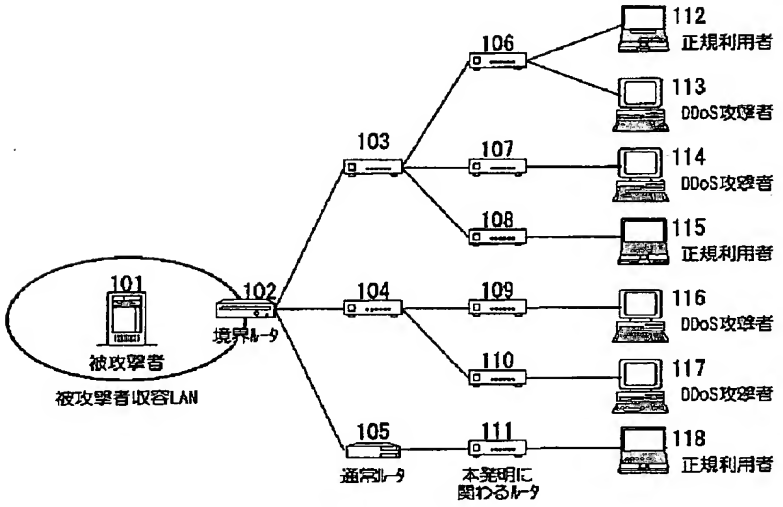
【図２６】　サービスモジュールの論理構造を示す概略図である。

【符号の説明】

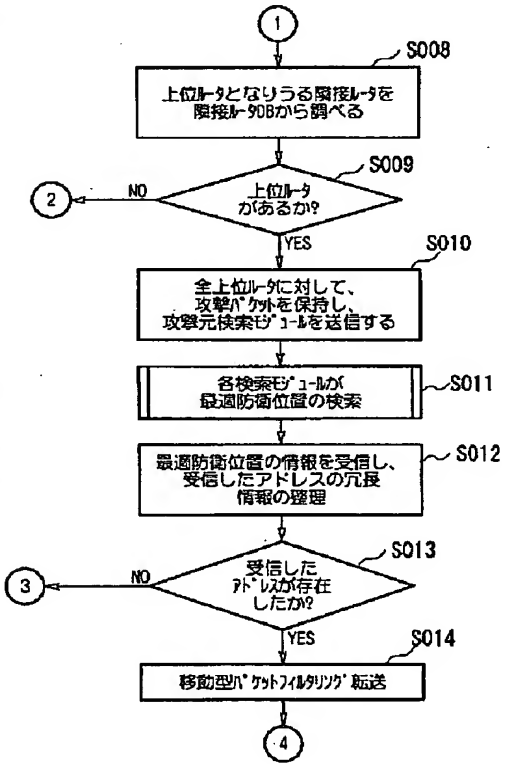
１　通信端末
２　中継ノード
３　モジュールサーバ
４　中継ノード
５　通信ネットワーク
６　中継ノード
７　通信端末
１１　サービスモジュール受信部
１２　認定開発者データベース
１３　サービスモジュールデータベース

１４　サービスメニュー
１５　サービスモジュールインジェクタ
１６　サービスマネージャ
１７　ユーザデータベース
２０　ノードカーネル
２１　実行エンジン
２２　サービスモジュール
１０１　被攻撃者のサーバ
１０２　境界ルータ
１０３，１０４，１０６～１１１　ルータ（本発明を適用したルータ）
１０５　ルータ（本発明を適用しないルータ）
１１２，１１５，１１８　正規利用者のコンピュータ
１１３，１１４，１１６，１１７　ＤｏＳ攻撃者のホスト

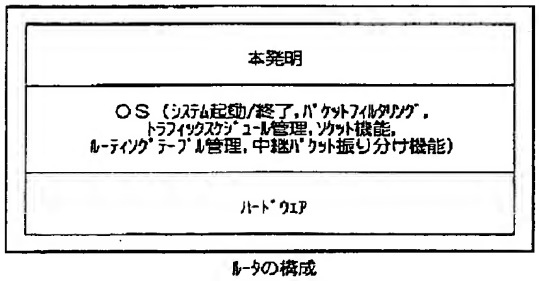
【図１】



【図４】

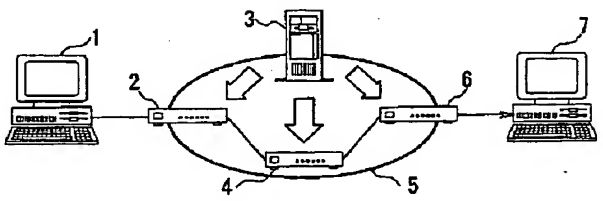


【図９】

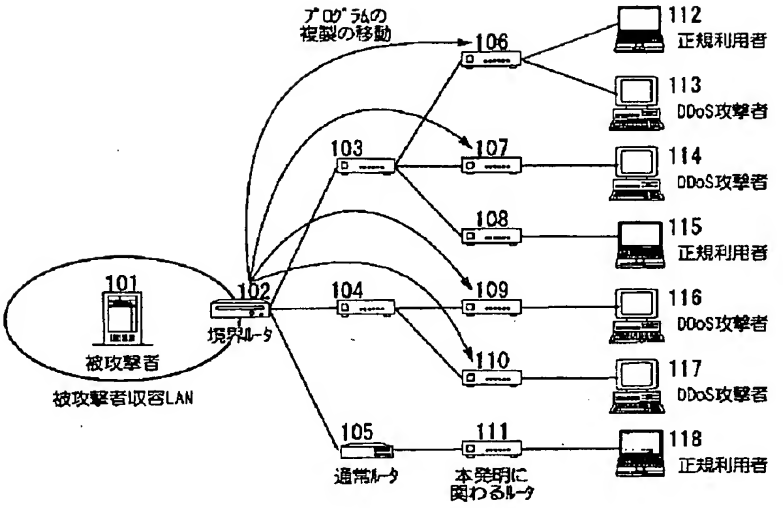


ルータの構成

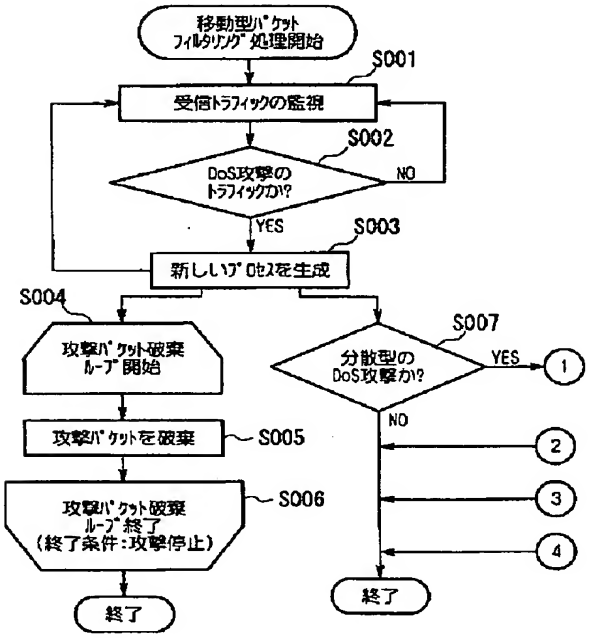
【図１９】



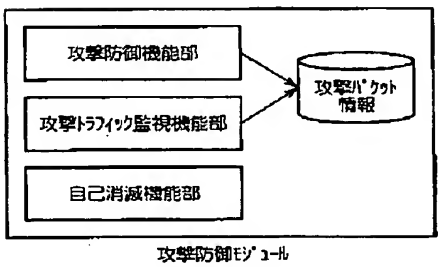
【図２】



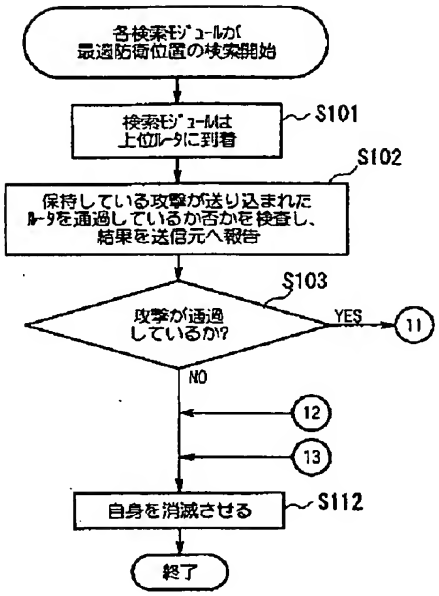
【図３】



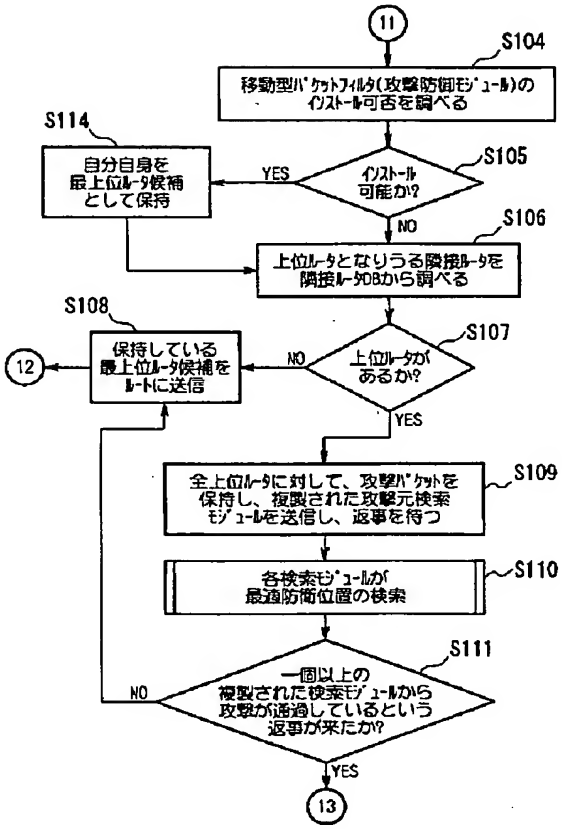
【図１２】



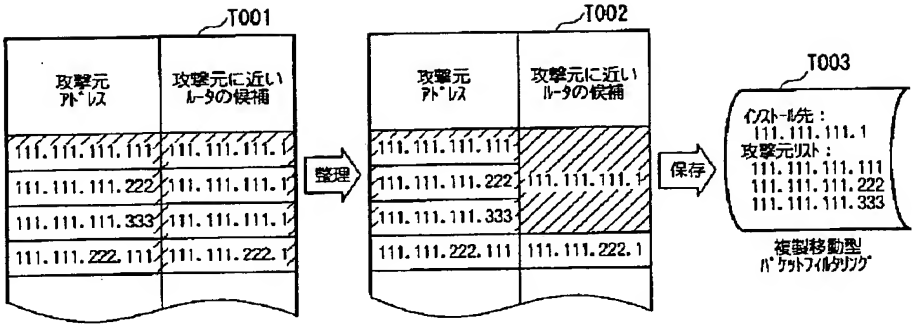
【図５】



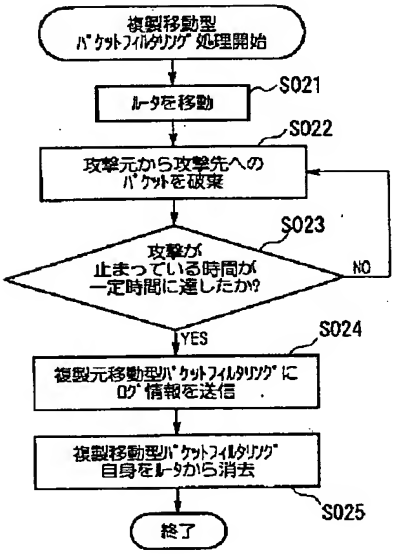
【図６】



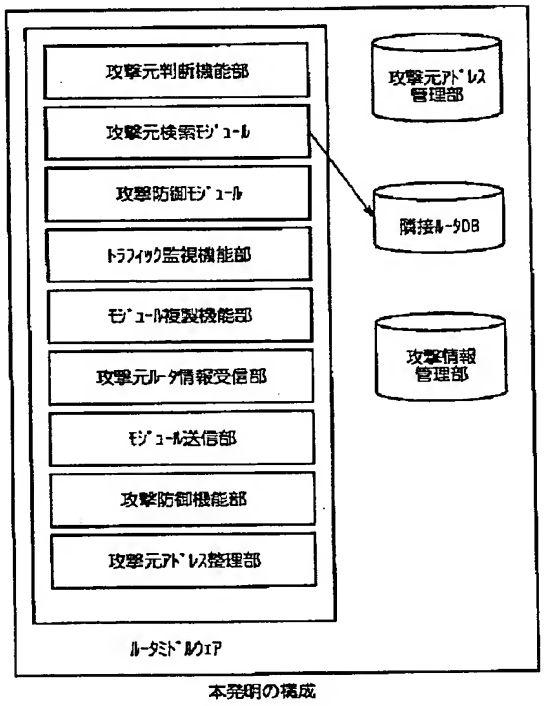
【図７】



【図８】

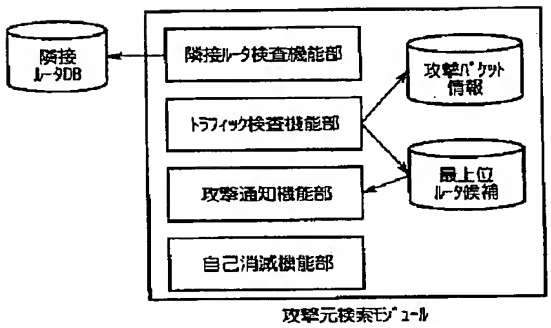


【図１０】



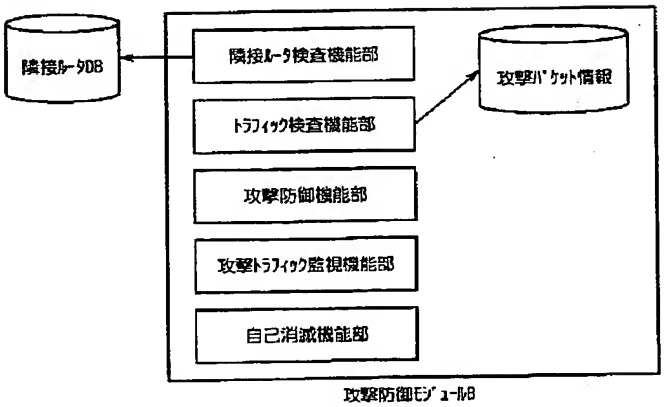
本発明の構成

【図１１】



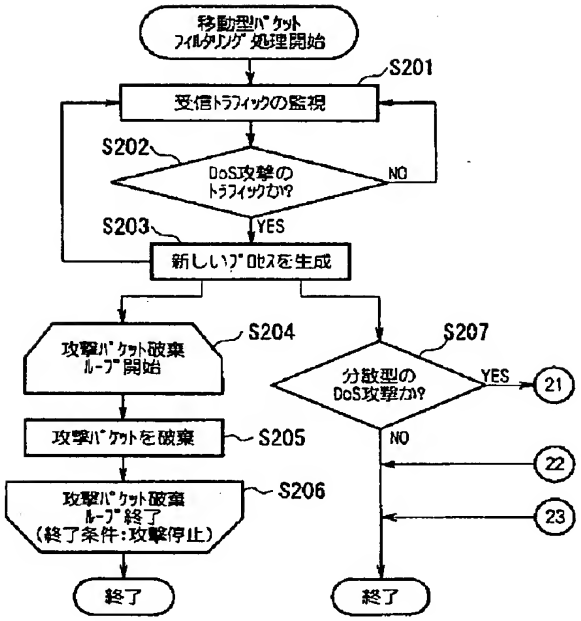
攻撃元検索ﾓｼﾞｭｰﾙ

【図１８】

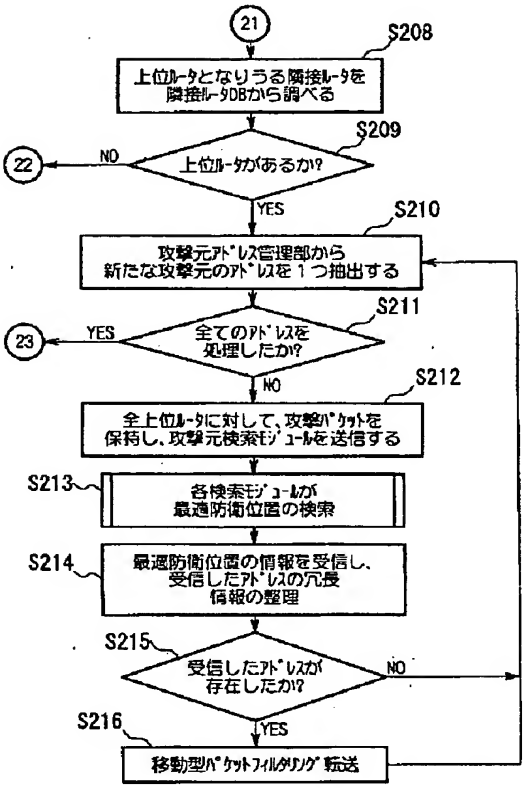


攻撃防御ﾓｼﾞｭｰﾙB

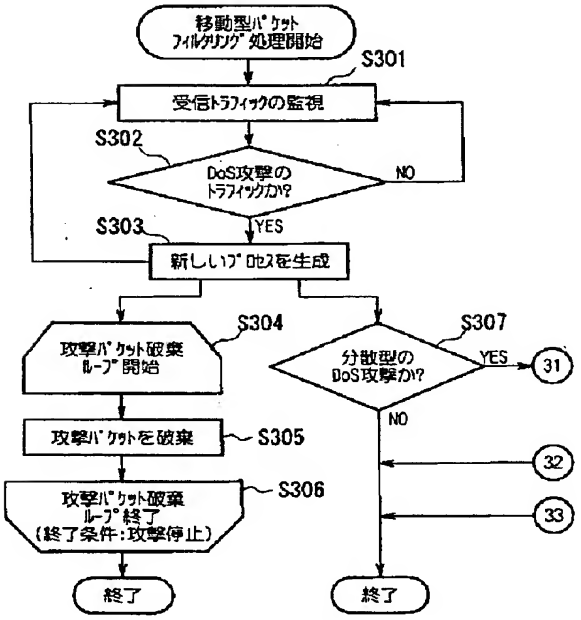
【図１３】



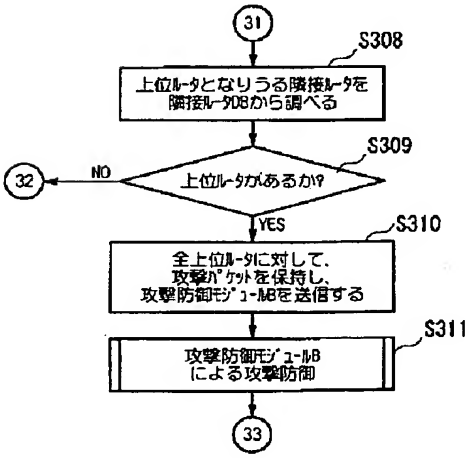
【図１４】



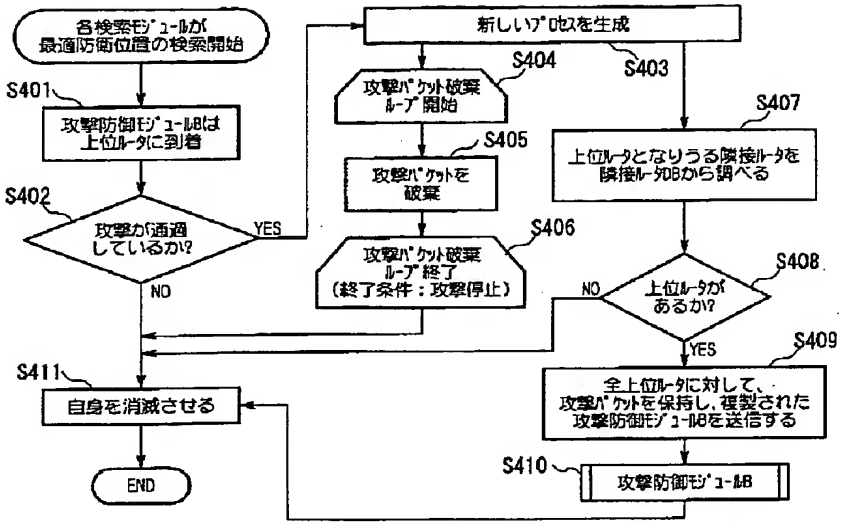
【図１５】



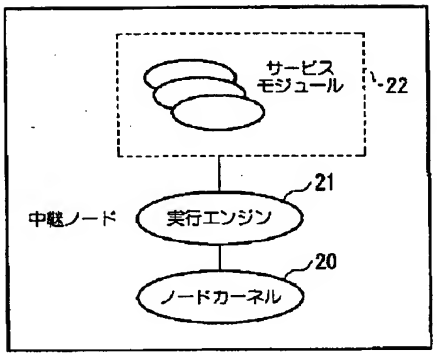
【図１６】



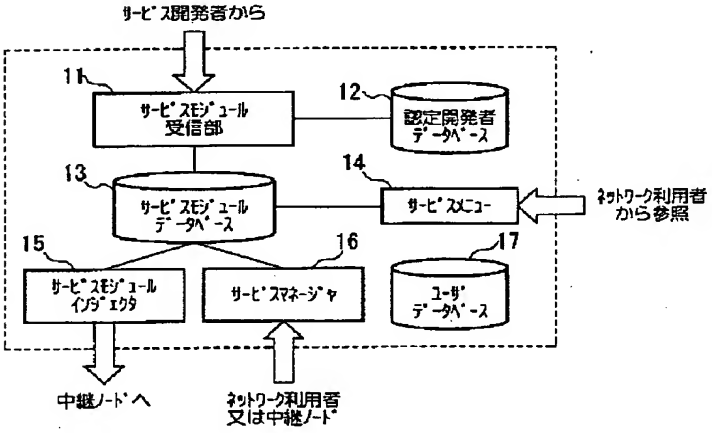
【図１７】



【図２１】



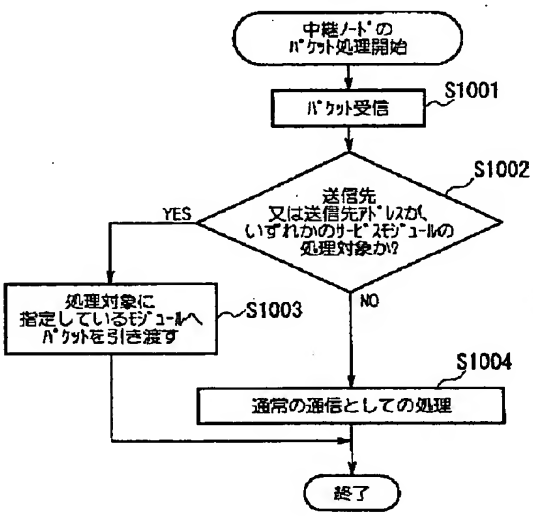
【図２０】



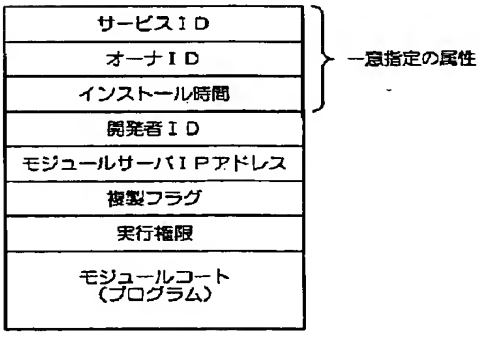
【図２２】

レイヤ	機能
実行エンジン	■ モジュール受信 ■ サービスマネージャ ■ モジュール実行ポリシ管理 ■ モジュール移動
ノードカーネル	■ システム起動／終了 ■ OS機能の隠蔽 （パケットフィルタリング、トラフィックスケジュール管理、socket管理、ルーティングテーブル管理等） ■ 受信パケットの振り分け

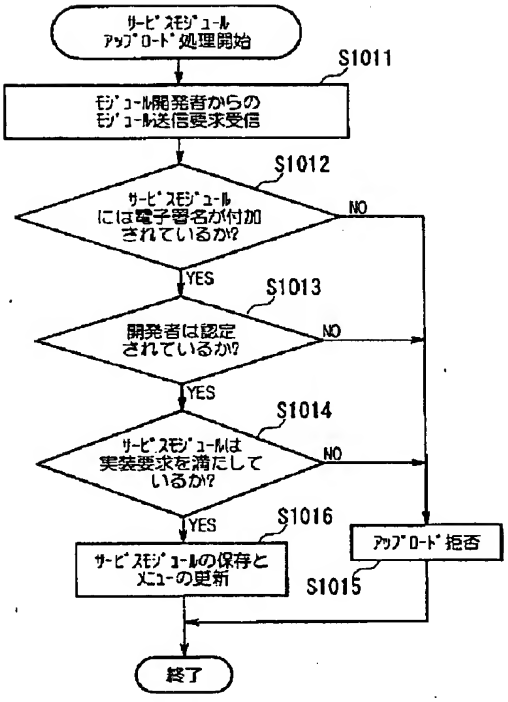
【図２３】



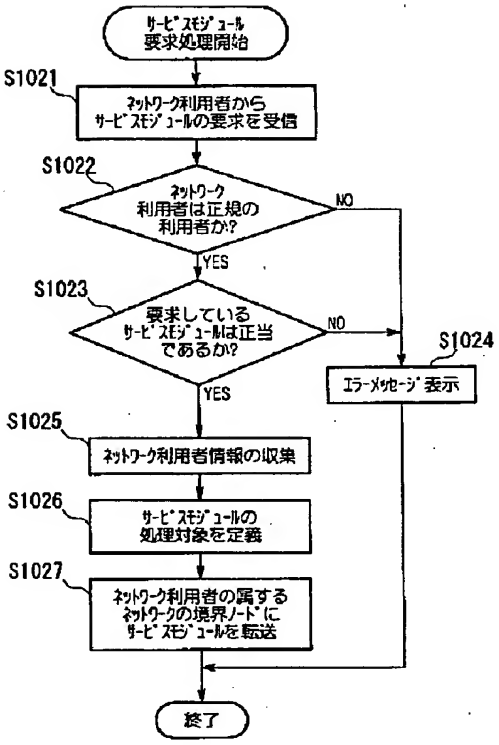
【図２６】



【図２４】



【図２５】



フロントページの続き

Ｆターム(参考) 5B089 GA11 GA21 GA31 GB02 KA17
KB06 KB13 KC54
5K030 GA15 HA08 HB19 HC01 HC14
HD03 HD06 LE01 MA01 MB09